

明 細 書

半導体メモリカード

技術分野

- [0001] 本発明は、主に、ネットワークを利用して映像・音声を録画・再生する映像音声信号処理端末に関する。

背景技術

- [0002] 近年、無線ネットワークインフラの普及に伴い、無線ネットワークを利用して映像や音声などのコンテンツを配信するサービスが普及してきている。無線ネットワークを介して配信されるコンテンツは、例えば無線ネットワークへの接続機能を有する端末によって受信され、記録媒体に格納される。無線接続機能を持つ端末としては、ユーザが移動しながら持ち歩くモバイル端末が典型的である。モバイル端末の一例としては、携帯電話やPDA(Personal Digital Assistance)、ノートブック型PC(Personal Computer)が挙げられる。
- [0003] モバイル端末には通常メモリカードなどの可搬型記録媒体が挿入され、コンテンツはそこに記録される。しかし、可搬型記録媒体の記憶容量には限りがあるため、映像や音声など情報量の多いコンテンツを大量に記録することができない。そこで、PCのハードディスクなどの大容量の記録媒体に接続した端末に可搬型記録媒体を挿入し、ハードディスクをコンテンツのバックアップ領域にすることも考えられる。この場合、可搬型記録媒体を端末と一体利用する必要があるため、モバイル端末としての用途の利便性を損ねてしまう。
- [0004] 本発明は、可搬型記録媒体において、モバイル端末が使用できる記録容量を拡大することを目的とする。また本発明は、無線ネットワークを介して配信されるコンテンツを、著作権に基づいて保護することを目的とする。さらに本発明は、任意のモバイル端末で利用可能な可搬型記録媒体を提供することを目的とする。
- ### 発明の開示
- [0005] 前記課題を解決するために、発明1は、電子機器に着脱可能な半導体メモリカードを提供する。この半導体メモリカードは、以下の要素を有している。

- ・書き換え可能な第1不揮発性メモリ、
- ・前記第1不揮発性メモリへの前記電子機器によるアクセスを制御する第1アクセス制御手段、
- ・書き換え可能な第2不揮発性メモリを有するネットワーク上の蓄積装置への前記電子機器によるアクセスを制御する通信手段、
- ・前記第2不揮発性メモリへの前記電子機器によるアクセスを制御する第2アクセス制御手段、
- ・前記第1不揮発性メモリ及び前記第2不揮発性メモリを含む擬似統合メモリ空間を生成する空間統合手段。

- [0006] 半導体メモリカードさえあれば任意の電子機器から蓄積装置にアクセスしてデータの書き込みや読み出しができるので、半導体メモリカードの見かけ上の記憶容量が増加する。従って、データ量の多いコンテンツ、例えば動画像データを記録するためのメモリ空間の自由度が高まり、ユーザの利便性を高めることができる。蓄積装置は、例えばデータベースとそのデータベースへの書き込みや読み出しを管理するDBMS(Data Base Management System)とを備えている。
- [0007] 発明2は、前記発明1において、前記第2アクセス手段によりアクセスしようとするデータが他の半導体メモリカードにより書込または読出中か否かを判断し、判断結果に応じて前記第2アクセス手段による書込及び／または読出を開始、中止または遅延させる競合判断手段をさらに備える半導体メモリカードを提供する。
- [0008] 編集処理とは、タイトルの変更や部分消去、明るさ調整など、既に存在している録画データの一部を変更する処理である。録画処理とは、新規に新しいデータを蓄積装置の第2不揮発性メモリに書き込む処理である。再生処理とは、既に存在している録画データを変更せずに読み出す処理である。複数のメモリカードから同一コンテンツへのアクセスを制御することにより、これから編集しようとしている対象のデータが他の半導体メモリカードからの蓄積装置へのアクセスによって書き換えられることを防止できる。また、これから再生しようとしている対象のデータが他の半導体メモリカードからの蓄積装置へのアクセスによって書き換えられることを防止することができる。さらに、これから再生しようとしている対象のデータが他の半導体メモリカードからの蓄積装

置への録画中である場合、既に録画されている部分から順次追っかけ再生することができる。

[0009] 発明3は、発明1において、前記通信手段が、前記蓄積装置の前記ネットワーク上でのアドレスを記憶している半導体メモリカードを提供する。電子機器は、記憶されたネットワークアドレスに基づいて、蓄積装置にアクセスすることができる。

[0010] 発明4は、前記発明3において、前記通信手段が、半導体メモリカードの識別情報を用いて前記蓄積装置にアクセスする半導体メモリカードを提供する。半導体メモリカードの識別情報により蓄積装置と半導体メモリカードとの間で相互認証を行うことができる。

[0011] 発明5は、前記発明1において、暗号化手段と認証手段とをさらに有する半導体メモリカードを提供する。暗号化手段は、前記データを暗号化するための暗号化キーを生成し、前記暗号化キーで前記データを暗号化する。認証手段は、前記電子機器の正当性を検証する。この半導体メモリカードにおいて、前記第1不揮発性メモリは、予め定められた記憶領域である第1認証領域と第1非認証領域とを含む。また、前記第1アクセス手段は、前記第1非認証領域への前記電子機器によるアクセスを制御する。さらに、前記第1アクセス手段は、前記認証手段が前記電子機器の正当性を認証した場合に、前記第1認証領域への前記電子機器によるアクセスを許可する。前記第2アクセス手段は、前記第2不揮発性メモリに含まれ予め定められた記憶領域である第2非認証領域への前記電子機器によるアクセスを制御する。前記空間統合手段は、前記第2不揮発性メモリ内の第2非認証領域のアドレスを前記暗号化キーで暗号化された前記データに割り当て、前記第1不揮発性メモリ内の第1認証領域のアドレスを前記暗号化キーに割り当てる。

[0012] 著作権で保護されているコンテンツを暗号化するための暗号化キーと暗号化コンテンツとを別々の場所に記憶する。たとえ暗号化コンテンツが不当に入手されたとしても、暗号化キーが同時に不当に入手されないので、暗号化コンテンツの解読が不可能となり、コンテンツのセキュリティを保証することができる。

[0013] 発明6は、前記発明5において、前記空間統合手段は、前記第1不揮発性メモリ内の第1非認証領域または前記第2不揮発性メモリ内の第2非認証領域のいずれのア

ドレスを前記暗号化キーで暗号化されたデータに割り当てるかを判断し、前記判断に従って前記データへのアドレスの割り当てを行う半導体メモリカードを提供する。

[0014] 第1非認証領域または第2非認証領域のいずれを割り当てるかの判断方法は、特に限定されない。いずれの判断方法を用いるかは、ユーザの利便性や記憶領域の効率性を考慮して決めることができる。例えば、空間統合手段は、半導体メモリカードまたは蓄積装置のどちらにデータを書き込むかの指示を、ユーザから受け付けても良い。その場合、統合手段は、ユーザからの指示に基づき、どちらの記憶領域のアドレスを暗号化データに割り当てるかを判断することができる。ユーザは、自分の使い勝手に合わせてデータを格納できるので便利である。別の方法として、空間統合手段は、どちらか一方に優先的に格納し、十分な空き領域がない場合に他方に格納するようにしても良い。例えば、空間統合手段は、第1不揮発性メモリ内の第1非認証領域に十分な空き領域があるかどうかを確認してもよい。その場合、統合手段は、その確認結果に基づいて第1非認証領域または第2非認証領域のいずれのアドレスを前記データに割り当てるかを判断することができる。データ量に応じてデータの格納先を選択するので、書き込み処理を効率化することができる。

[0015] 発明7は、前記発明5において、前記第2アクセス手段が、前記認証手段が前記電子機器の正当性を認証した場合、前記第2不揮発性メモリ内の予め定められた記憶領域である前記第2認証領域への前記電子機器によるアクセスを許可する半導体メモリカードを提供する。

[0016] 第2認証領域を蓄積装置に設けることにより、半導体メモリカード中の第1認証領域をも見かけ上増大させることができる。従って、例えばコンテンツなどのデータを暗号化せずに第1または第2認証領域に格納しても、記憶領域を十分に準備でき、かつコンテンツのセキュリティを保證することができる。

[0017] 発明8は、前記発明1において、前記第1不揮発性メモリは管理領域を含む半導体メモリカードを提供する。ここで、前記空間統合手段は、前記第1不揮発性メモリまたは前記第2不揮発性メモリ中のアドレスをデータに割り当て、前記データを識別するデータ識別子と前記割り当てたアドレスと対応づけて前記管理領域に書き込む。前記第1アクセス手段及び前記第2アクセス手段は、前記第1不揮発性メモリまたは前

記第2不揮発性メモリへの前記データの書き込み要求を受け付け、前記データに割り当てられたアドレスに対応する記憶領域に前記データを書き込む。

- [0018] 管理領域はいわゆるFATに相当する。第1不揮発性メモリ内のFATは、第1不揮発性メモリ内の第1認証領域及び第1非認証領域のアドレスと、第2不揮発性メモリ内の第2非認証領域のアドレスとを管理する。例えば、空間統合手段は、第1認証領域及び第2非認証領域にアドレス0000〜3FFFを割り当て、第2非認証領域にアドレス4000〜FFFFを割り当てる。第1認証領域、第1非認証領域または第2非認証領域に書き込まれるデータの識別子は、空間統合手段が管理するいずれかのアドレスと対応づけてFATに記憶される。このようにして、空間統合手段は、擬似的な統合メモリ空間を生成することができる。
- [0019] 発明9は、前記発明8において、前記第2アクセス手段は、データの読み出し要求を受け付け、前記データが書き込まれている第2不揮発性メモリのアドレスを前記管理領域から読み出し、読み出したアドレスに前記通信手段を介してアクセスして前記データを読み出す半導体メモリカードを提供する。
- [0020] 電子機器のユーザから読み出し要求を受けた場合、第2アクセス手段は、データが第2非認証領域に蓄積されていれば、データ識別子に対応するアドレスにアクセスして第2非認証領域からデータを読み出す。これにより、ユーザは、半導体メモリカードさえあれば、コンテンツなどのデータを半導体メモリカードからはもちろん、蓄積装置からも読み出すことができる。
- [0021] 発明10は、前記発明8において、前記データを暗号化及び復号化するための暗号化キーを生成し、前記暗号化キーで前記データを暗号化する暗号化手段をさらに有する半導体メモリカードを提供する。この発明において、前記第2アクセス手段は、前記暗号化キーで暗号化されたデータが書き込まれている前記第2非認証領域のアドレスを前記管理領域から読み出し、前記第2非認証領域の前記アドレスにアクセスして暗号化された前記データを前記通信手段を介して読み出す。前記第1アクセス手段は、前記暗号化キーが書き込まれている第1認証領域のアドレスを前記管理領域から読み出し、前記第1認証領域の前記アドレスにアクセスして前記暗号化キーを読み出す。

[0022] 著作権で保護されているコンテンツを暗号化するための暗号化キーと暗号化コンテンツとを別々の場所に記憶する。たとえ暗号化コンテンツが不当に入手されたとしても、暗号化キーが同時に不当に入手されないので、暗号化コンテンツの解読が不可能となり、コンテンツのセキュリティを保証することができる。

[0023] 発明11は、下記のステップを含むメモリ空間管理方法を提供する。

- ・書き換え可能な第1不揮発性メモリへの電子機器によるアクセスを制御する第1アクセス制御ステップ、
- ・書き換え可能な第2不揮発性メモリを有するネットワーク上の蓄積装置への前記電子機器によるアクセスを制御する通信ステップ、
- ・前記第2不揮発性メモリへの前記電子機器によるアクセスを制御する第2アクセス制御ステップ、
- ・前記第1不揮発性メモリ及び前記第2不揮発性メモリを含む擬似統合メモリ空間を生成する空間統合ステップ。

[0024] この方法は、前記発明1と同様の作用効果を奏する。

[0025] 発明12は、電子機器に着脱可能でありコンピュータを含む半導体メモリカードに記録されたメモリ空間管理プログラムを提供する。このプログラムは、前記コンピュータを下記の手段として機能させる。

- ・書き換え可能な第1不揮発性メモリへの前記電子機器によるアクセスを制御する第1アクセス制御手段、
- ・書き換え可能な第2不揮発性メモリを有するネットワーク上の蓄積装置への前記電子機器によるアクセスを制御する通信手段、
- ・前記第2不揮発性メモリへの前記電子機器によるアクセスを制御する第2アクセス制御手段、
- ・前記第1不揮発性メモリ及び前記第2不揮発性メモリを含む擬似統合メモリ空間を生成する空間統合手段。

[0026] このプログラムは、前記発明1と同様の作用効果を奏する。また、このプログラムを記録したコンピュータ読み取り可能な記録媒体も本発明に含まれる。ここで、記録媒体としては、コンピュータが読み書き可能なフレキシブルディスク、ハードディスク、半

導体メモリ、CD-ROM、DVD、光磁気ディスク(MO)、その他のものが挙げられる。またプログラムには、記録媒体に記憶されているものもダウンロード可能なものが含まれる。

図面の簡単な説明

- [0027] [図1]メモ리카ードが挿入された端末を含むシステム
[図2]メモ리카ードの機能構成を示すブロック図
[図3]NV-RAMに記憶されている接続情報の一例
[図4]一覧データの概念説明図
[図5]図4の一覧データに基づいて表示される録画済番組の一覧表示画面例
[図6]空間統合部が書込を行うFATに記録される情報の概念説明図
[図7]空間統合部が行うアドレス変換の概念説明図
[図8]端末の構成図
[図9]接続処理の流れの一例を示すフローチャート
[図10A]書込処理の流れの一例を示すフローチャート
[図10B]書込処理の流れの一例を示すフローチャート(メモ리카ード側の一部)
[図11]一覧出力処理の流れの一例を示すフローチャート
[図12]読出処理の流れの一例を示すフローチャート
[図13]排他制御処理の流れの一例を示すフローチャート
[図14]アクセス権管理がある場合の番組一覧表示画面例
[図15]ストレージサーバが保持するアクセス権管理テーブルのデータ例
[図16]ストレージサーバに対し、異なるアクセス権でアクセス可能なメモ리카ードを作成するための画面例

発明を実施するための最良の形態

[0028] <発明の概要>

本発明の半導体メモ리카ード(以下、単にメモ리카ードという)は、電子機器に挿入され、データの書込や読み出しが行われる。メモ리카ードは、書込や読み出しを行う電子機器の認証が必要な認証領域(第1認証領域に相当)と認証が不要な非認証領域(第1非認証領域に相当)とを有している。本発明のメモ리카ードは、無線ネットワーク

接続手段を有し、これによりネットワーク上のストレージサーバ(蓄積装置に相当)に電子機器をアクセスさせる。ストレージサーバには少なくとも非認証領域(第2非認証領域に相当)が設けられている。

[0029] コンテンツなどのデータは、メモ리카ードの非認証領域またはストレージサーバの非認証領域に書き込まれる。言い換えれば、ストレージサーバの非認証領域の分だけ、データを書き込める記憶領域が広がる。従って、見かけ上はメモ리카ードの非認証領域が増大したように見える。

[0030] また、著作権などで保護されているコンテンツの暗号化及び復号化に用いられる暗号化キーは、メモ리카ード上の認証領域に書き込まれる。ストレージサーバ上の非認証領域にあるコンテンツデータには誰でもアクセスできても、そのコンテンツを復号化するために必要な暗号化キーはメモ리카ード内にある。結局、メモ리카ード及び正当な電子機器を有している者だけが、暗号化キーによりコンテンツを復号化・再生出力することができる。従って、メモ리카ードの記憶容量を見かけ上増大しつつ、著作権などで保護されたデータのセキュリティを保証することができる。

[0031] <第1実施形態>

図1は、本発明のメモ리카ード13が挿入された端末14を含むシステム10の一例を示す。このシステム10は、ストレージサーバ11、無線ネットワークの基地局12、メモ리카ード13、メモ리카ード13が挿入された端末14(電子機器に相当)及び出力装置15を含む。出力装置15は、音声や画像を出力するためのスピーカやディスプレイなどである。ストレージサーバ11と基地局12とはネットワーク106により接続されている。基地局12とメモ리카ード13とは、無線ネットワークにより接続可能である。以下、メモ리카ード13及びストレージサーバ11の構成について、さらに詳細に説明する。

[0032] [メモ리카ード]

(1)全体構成

図2は、メモ리카ード13の機能構成を示すブロック図である。メモ리카ード13は、電源供給端子131を介して外部からの電源と、クロック信号の供給とを受けて動作する。また、メモ리카ード13は、データI/O端子132によって端末14などの外部機器と電氣的に接続される。このほかに、メモ리카ード13はさらに以下の要素(a)〜(h)を有し

ている。

[0033] (a) 無線通信部(通信手段に相当)

無線通信部133は、基地局12を介してメモリカード13とネットワーク106とを接続する。接続には、後述するNV-RAM136に記憶された接続情報が用いられる。

[0034] (b) ROM

ROM134は、マスタ鍵及び各種プログラムを記憶している。各種プログラムは、後述するCPU137により実行され、各種機能を達成する。マスタ鍵は、端末14やストレージサーバ11との相互認証の際に用いられる。また、マスタ鍵は、フラッシュメモリ139やストレージサーバ11内のデータの保護にも用いられる。

[0035] (c) RAM

RAM135は、CPU137が処理を行う際の作業領域として用いられる。

[0036] (d) NV-RAM

NV-RAM136は、ストレージサーバ11に接続するために必要な接続情報を記憶している不揮発性メモリである。接続情報としては、例えば、ストレージサーバ11のネットワークアドレスが挙げられる。図3は、NV-RAM136に記憶されている接続情報の一例を示す。この例では、ストレージサーバ11のURL、接続用識別ID及び接続認証パスワードが接続情報に含まれている。接続用識別ID及び接続認証パスワードは、メモリカード13を識別する識別情報である。

[0037] (e) CPU

CPU137は、ROM134に記憶されている各種プログラムを実行し、各種機能を達成する。

[0038] (f) 特殊領域(ROM)

特殊領域138は、メモリカード13に固有の識別情報であるメディアIDやこのメモリカード13の製造メーカー名等の情報を予め記憶している。メディアIDは、他の半導体メモリカード13と区別してメモリカード13を識別することが可能な固有の識別子である。本実施形態では、メディアIDは、機器間の相互認証に用いられ、認証領域への不正なアクセス及びストレージサーバ11への不当なアクセスを防止するために使用される。

[0039] (g)フラッシュメモリ(第1不揮発性メモリに相当)

フラッシュメモリ139は、何度も繰り返して書き込みが行える書き換え可能な不揮発性メモリである。フラッシュメモリ139は、論理的な記憶領域として、FAT(管理領域に相当)139aと、認証領域(第1認証領域に相当)139bと、非認証領域(第1非認証領域に相当)139cと、を有する。認証領域139bは、正当な機器であると認証された端末14だけがアクセスできる記憶領域である。非認証領域139cは、そのような認証を必要とすることなく端末14がアクセスできる記憶領域である。FAT139aは、フラッシュメモリ139及びストレージサーバ11内の記憶領域を含むメモリ空間を統一的に管理するための記憶領域である。

[0040] 認証領域139bは、著作権保護に関わる重要なデータを格納するために用いられる。認証領域139bは、端末14とメモリカード13との間で認証が成功した時にのみ読み書きができる領域である。認証領域139bへのアクセスには、暗号化されたコマンドが用いられる。認証領域139bには、例えばパスワードを暗号化した暗号化キーや読出回数が記憶される。パスワードは、著作権で保護されたデータを暗号化するのに用いられる。読出回数は、前記データを再生したりデジタル出力したり出来る回数を示す。なお、図示していないが、暗号化キーや読出回数は、データIDと対応付けて記憶され、データIDをキーに検索可能である。

[0041] 非認証領域139cは、一般的なコンピュータシステムにおける補助記憶装置として用いられる。非認証領域139cは、ATAやSCSI等の公開されたコマンドでアクセスできる、即ち認証せずに読み書きできる領域である。従って、非認証領域139cに対しては、フラッシュATAやコンパクトフラッシュ(登録商標)と同じように、端末14上のファイル管理ソフトウェアでデータの読み書きが可能である。非認証領域139cには、例えば前記パスワードで暗号化された暗号化コンテンツや一覧データが記憶される。図4は、一覧データの概念図である。この図では、一例として、録画済番組の一覧を出力するための一覧データを示している。図5は、図4の一覧データに基づいて表示される録画済番組の一覧表示画面例である。この画面は、任意の番組の読み出し処理要求を受け付ける。

[0042] 前記認証領域139b及び非認証領域139cに記憶されている情報はほんの一例で

あり、ここに挙げた例に限定されない。

[0043] (h)暗号・復号化回路

暗号・復号化回路1310は、データの暗号化及び復号化を行う制御回路である。暗号・復号化回路1310は、フラッシュメモリ139にデータを書き込む際にそのデータを暗号化して書き込み、フラッシュメモリ139からデータを読み出した際にそのデータを復号化する。これは、不正なユーザがこのメモリカード13を分解してフラッシュメモリ139の内容を直接解析し、認証領域に格納された暗号化キーなどを盗む等の不正行為を防止するためである。

[0044] (2)CPUの機能

ROM134に記憶されたプログラムは、CPU137に以下の機能を達成させる。なお、本実施形態ではプログラムにより以下の機能を実現しているが、以下の機能をアクティブ素子からなる制御回路でハードウェア的に実現することも可能である。

[0045] (2-1)認証部

ROM134に記憶された認証プログラムは、メモリカード13のCPU137を認証部(認証手段に相当)として機能させる。認証部は、メモリカード13にアクセスしようとする端末14とチャレンジ・レスポンス型の相互認証を行う。認証部は、乱数発生プログラムや暗号プログラム等を有し、その暗号プログラムと同一の暗号プログラムを端末14が有しているか否かを検出することによって、端末14の正当性を認証する。なお、チャレンジ・レスポンス型の相互認証とは、メモリカード13から端末14に送ったチャレンジデータと、端末14からメモリカード13に送られたレスポンスデータとを比較することで、端末14を認証することができるか否かを判断するという認証ステップを、双方の機器が相互に行う認証方法である。認証ステップでは、メモリカード13は端末14の正当性を検証するためのチャレンジデータを端末14に送る。それに対して端末14は、自己の正当性を証明する処理を施こしてレスポンスデータを生成し、メモリカード13に送る。

[0046] (2-2)コマンド判定部

ROM134に記憶されたコマンド判定プログラムは、メモリカード13のCPU137をコマンド判定部として機能させる。コマンド判定部は、メモリカード13への命令であるコ

マンドの種類を判定する。コマンドには、フラッシュメモリ139及びストレージサーバ11のデータを読み・書き・消去するコマンドが含まれる。このようなコマンドは、データI/O端子132を介して入力される。入力されたコマンドの種類に応じて、以下に述べる各種機能部が動作する。

[0047] (2-3) アクセス制御部

ROM134に記憶されたアクセス制御プログラムは、メモリカード13のCPU137をアクセス制御部(第1アクセス手段及び第2アクセス手段に相当)として機能させる。アクセス制御部は、それぞれ、フラッシュメモリ139の認証領域139b及び非認証領域139cへのデータの書き込み及び読み出しを実行する。認証領域139bへの書込依頼や読込依頼は、認証部により認証された端末14からの依頼のみ許可される。

[0048] また、アクセス制御部は、後述するストレージサーバ11の非認証領域(第2非認証領域に相当)111へのデータの書き込み及び読み出しを実行する。書き込み及び読み出しの具体的な方法としては、例えば次のようなものが挙げられる。ストレージサーバ11と無線通信部133とがHTTP(HyperText Transfer Protocol)により通信可能である場合を考える。読み出しの場合、アクセス制御部は無線通信部133を介してGETコマンド及びRANGE指定子を利用することにより、ストレージサーバ11上の指定アドレスからデータを読み出すことができる。書き込みの場合、アクセス制御部はPUSHコマンド/POSTコマンド及びRANGE指定子を利用することにより、ストレージサーバ11上の指定アドレスに対してデータを書き込むことが出来る。もちろん、ストレージサーバ11と無線通信部133との通信は、HTTPに限定されない。例えばFTP(File Transfer Protocol)など、他の通信プロトコルを用いても構わない。

[0049] なお、データの書込処理には録画処理と編集処理とが含まれる。また、データの読出処理には再生処理と追っかけ再生処理とが含まれる。録画処理とは、新規に新しいデータを記憶領域に書き込む処理である。編集処理とは、タイトルの変更や部分消去、明るさ調整など、既に存在するデータの一部を変更する処理である。再生処理とは、既に存在しているデータを変更せずに出力する処理である。追っかけ再生処理とは、データの書込アドレスがデータの読出アドレスを追い越さない範囲で、既に存在しているデータを変更せずに出力する処理である。この他に、データの読出

処理には、データのデジタル出力、例えばコピーや移動を含んでいてもよい。

[0050] (2-4) 空間統合部

ROM134に記憶された空間統合プログラムは、メモ리카ード13のCPU137を空間統合部(空間統合手段に相当)として機能させる。空間統合部は、フラッシュメモリ139の認証領域139b及び非認証領域139cと、ストレージサーバ11の非認証領域111と、を含む擬似統合メモリ空間を生成する。

[0051] 図6は、空間統合部が書込を行うFAT139aに記録される情報の概念説明図である。FAT139aは、フラッシュメモリ139内にされる、アドレス管理用の記録領域である。FAT139aには、フラッシュメモリ139の認証領域139b及び非認証領域139cのアドレスと、ストレージサーバ11の非認証領域111のアドレスとが記憶されている。言い換えれば、FAT139aには、擬似統合メモリ空間のアドレスが記憶されている。いずれかの記憶領域に書き込まれたデータの識別子は、そのデータが書き込まれたアドレスと対応付けてFATに記憶される。例えば、データID「ENCRYPT/MOV00011.MPG」は、アドレス0000〜0099に対応付けて記憶されている。これは、このデータIDで特定されるコンテンツが、アドレス0000〜0099に蓄積されていることを示す。

[0052] この例では、空間統合部は、フラッシュメモリ139の認証領域139b及び非認証領域139cにアドレス0000〜3999を割り当て、ストレージサーバ11の非認証領域111にアドレス4000〜9999を割り当てている。各記憶領域139b、139c、111の境界線の位置は、空間統合部により図示しないバッファなどに書き込まれる。境界線の位置は、固定であっても良いし、可変でも良い。この図では、「ENCRYPT/MOV00011.MPG」及び「ENCRYPT/MOV00012.MPG」で識別されるデータは、認証領域139bに記憶されている。また、「DVD#RTAV/MOV00011.MPG」で識別されるデータは、非認証領域139cに記憶されている。さらに、「DVD#RTAV/MOV00012.MPG」で識別されるデータは、ストレージサーバ11の非認証領域111に記憶されている。

[0053] 端末14からの読み出し依頼に応じてデータを読み出すときは、空間管理部は、FAT139aを参照してフラッシュメモリ139またはストレージサーバ11のどちらに蓄積され

ているデータなのかを判断し、判断結果及びアドレスをアドレス制御部に渡す。

- [0054] 図7は、空間統合部が行うアドレス変換の概念説明図である。ストレージサーバ11の非認証領域111にアクセスしているように見せかけるために、ストレージサーバ11に対する書き込みや読み出しの際にはアドレス変換が必要となる。書き込みや読み出しは、RAM135内のバッファ135aを作業領域に用いて行われる。この図は、ストレージサーバ11の非認証領域111中のアドレス4000〜4399に記憶された399Mバイトのデータファイルを読み出す場合のアドレス変換を示す。バッファは、最大100Mバイトのデータを蓄積可能であり、0〜99のアドレスが割り当てられている。データファイルは、例えば100MバイトずつRAM135中のバッファに一時保存される。データファイルの先頭の100Mバイトがバッファに書き込まれると、空間統合部はバッファのアドレスを0〜99から4000〜4099に変換する。このアドレスとデータとは端末14に返される。次の100Mバイトが書き込まれると、空間統合部はバッファのアドレスを4100〜4199に変換し、アクセス制御部はアドレスとデータとを端末14に返す。これをデータファイルの終わりまで繰り返すことで、端末14側では見かけ上アドレス4000〜4399にアクセスしたように見える。ストレージサーバ11にデータを書き込むときには、逆の処理が行われる。

- [0055] このように、FATによりフラッシュメモリ139とストレージサーバ11内の記憶領域とを1つにまとめて管理することにより、擬似的な統合メモリ空間を生成し、フラッシュメモリ139の記憶容量を見かけ上増大させることができる。著作権で保護されるコンテンツは、通常は暗号化された後にフラッシュメモリ139の非認証領域139bに格納されるので、非認証領域111をストレージサーバ11に設けることにより、フラッシュメモリ139の記憶容量を見かけ上増大させることができる。従って、動画像データなどデータ量の多いコンテンツを記録するためのメモリ空間の自由度が高まり、ユーザの利便性を高めることができる。

- [0056] (2-5) 接続部

ROM134に記憶された接続プログラムは、メモ리카ード13のCPU137を接続部(通信手段の一部に相当)として機能させる。接続部は、NV-RAM136に記憶された接続情報を用い、無線通信部133を介してストレージサーバ11への接続を行う。

[0057] (2-6) 競合判断部

ROM134に記憶された競合判断プログラムは、メモ리카ード13のCPU137を競合判断部(第1, 第2及び第3競合判断手段に相当)として機能させる。競合判断部は、他のメモ리카ード13が同一のアクセス対象にアクセスしている場合に、矛盾が発生することを防止する。具体的には、競合判断部は、書込をしようとしている対象のデータが、他のメモ리카ード13の書込対象となっている場合、書込に一定の制限を加える。また、競合判断部は、読み出そうとしている対象のデータが、他のメモ리카ード13の書込対象となっている場合、読出に一定の制限を加える。

[0058] [端末]

図8は、端末14の構成図を示す。端末14は、RAM141、マイクロプロセッサ142、媒体入出力部143、ハードディスクユニット144及び映像信号出力部145が、内部バス146を介して接続されて構成されている。ハードディスクユニット144は、プログラムを記憶している。このプログラムに従ってマイクロプロセッサ142が動作することにより、端末14を構成する各処理部はその機能を達成する。ハードディスクユニット144には、非認証領域111が形成される。非認証領域111は、メモ리카ード13上の非認証領域139cと同様に、番組データや一覧データを記憶している。

[0059] [処理]

次に、本実施形態のメモ리카ード13及びそのメモ리카ード13を挿入した端末14が行う処理について、図面を参照して具体的に説明する。処理は、大別して(1)接続処理、(2)書込処理、(3)一覧出力処理、(4)読み出し処理、(5)排他制御処理に分けることが出来る。以下、これら(1)〜(5)の処理についてそれぞれ説明する。以下の説明においては、著作権で保護された番組データ(以下、コンテンツという)の書込や読出・読出に伴う一覧出力処理を行う場合を例に取る。また、以下の説明で用いる図8〜図12において、メモ리카ード13をRMと略している場合がある。

[0060] (1) 接続処理

図9は、メモ리카ード13を端末14に挿入したときに実行される接続処理の流れの一例を示すフローチャートである。以下の処理により、メモ리카ード13は基地局12を通じてネットワークに接続を試みる。以下の処理は、メモ리카ード13を端末14に挿入す

ることにより開始される。

- [0061] ステップS101:電源供給端子131を介し、外部からメモ리카ード13に電力が供給される。
- [0062] ステップS102〜S103:電力の供給をきっかけに、ROM134に記憶されている接続プログラムがCPU137に読み込まれ、起動される(S102)。接続部としてのCPU137は、NV-RAM136に記憶されている接続情報を読み出し(S103)、これに基づいて無線通信部133を介してストレージサーバ11への接続を試みる。
- [0063] ステップS104〜S105:CPU137の接続部は、無線ネットワークが利用可能か否かを判断する(S104)。利用可能でない場合には、「ネットワーク接続待機モード」に移行する(S105)。ネットワーク接続待機モード中は、接続部は、例えば一定時間毎に継続的に無線ネットワークが利用可能になったか否かを確認する。またその一方で、接続部は、既にRAM135にダウンロードされているストレージサーバ11中のコンテンツに限り、ストレージサーバ11中のコンテンツへのアクセスを行う。
- [0064] ステップS106:無線ネットワークが利用可能な場合、接続部は無線通信部133を介してストレージサーバ11に接続する。
- [0065] ステップS107:さらに接続部は、接続情報を利用してストレージサーバ11との認証を行い、接続を確立する。
- [0066] ステップS108〜S109:接続部は、ストレージサーバ11に同時にアクセスするメモ리카ード13が他にあるか否かを判断する。この判断は、ストレージサーバ11側に同時接続数を問い合わせ得られる応答に基づいて行うことが出来る。他のメモ리카ード13から同時に非同期なアクセスが発生する場合には、これら非同期アクセスによる矛盾を防ぐために、排他制御モードに移行する(S109)。具体的には、接続部は、録画及び編集が可能であることを示す録画処理許可フラグ及び編集処理許可フラグを、それぞれ「OFF」に設定する。また、接続部は、再生及び追っかけ再生が可能であることを示す再生処理許可フラグ及び追っかけ再生処理許可フラグを、それぞれ「OFF」に設定する。
- [0067] ステップS110:接続部は、ストレージサーバ11にアクセスする他のメモ리카ード13がない場合、ファイルアクセスモードを設定する(S110)。具体的には、接続部は、録

画及び編集が可能であることを示す録画処理許可フラグ及び編集処理許可フラグを、それぞれ「ON」に設定する。また、接続部は、再生及び追っかけ再生が可能であることを示す再生処理許可フラグ及び追っかけ再生処理許可フラグを、それぞれ「ON」に設定する。

[0068] 以上の処理により、メモリカード13とストレージサーバ11との接続を確立することができる。また、他のメモリカード13と競合する場合には、どの処理が競合するのかをメモリカード13が把握することができる。

[0069] (2) 書込処理

図10A, 10Bは、端末14がコンテンツをメモリカード13に書き込むときに、端末14及びメモリカード13が実行する処理の流れの一例を示すフローチャートである。

[0070] (2-1) 端末側の処理

端末14のユーザが画面上の所定のボタンを押下するなどによりデータの書込処理を指示すると、端末14では以下の処理が開始される。以下の処理では、端末14はメモリカード13に対し、コンテンツの書込要求を行う。

[0071] ステップS201: 端末14のマイクロプロセッサ142は、画面上の所定のボタンの押下などによる書込要求を受け付ける。

[0072] ステップS202: 端末14のマイクロプロセッサ142は、メモリカード13の認証プログラムとチャレンジ・レスポンス型の認証を行う。

[0073] ステップS203: 端末14のマイクロプロセッサ142は、メモリカード13との認証処理に成功すると、メモリカード13に対してマスタ鍵及びメディアIDの読み出しを依頼し、これらを取得する。

[0074] ステップS204: 端末14のマイクロプロセッサ142は、乱数を生成し、メモリカード13から取得したマスタ鍵とメディアIDと生成した乱数とから、コンテンツを暗号化するためのパスワードを生成する。このときの乱数は、例えば、上記認証において、メモリカード13に送信したチャレンジデータ(乱数)を暗号化したもの等である。

[0075] ステップS205: 端末14のマイクロプロセッサ142は、得られたパスワードをマスタ鍵とメディアIDとで暗号化し、暗号化キーを生成する。さらにマイクロプロセッサ142は、生成した暗号化キーを認証領域139bに書き込むようメモリカード13に依頼し、暗号

化キーを認証領域139bに格納する。この依頼は、暗号化キーを送信するのに先立ち、認証領域139bに書き込むためのコマンドを暗号化してメモリカード13に送信することにより行う。

[0076] ステップS206: 端末14のマイクロプロセッサ142は、コンテンツをパスワードで暗号化しながら暗号化コンテンツをメモリカード13に渡し、書込を依頼する。

[0077] 以上の端末14側における書込処理は、ストレージサーバ11上に非認証領域111が設けられていない場合と同じである。

[0078] (2-2)メモリカード側の処理

再び図10を参照し、メモリカード13側における書込処理の流れの一例について説明する。この処理では、端末14からの書込要求に応じ、メモリカード13またはストレージサーバ11のいずれかにコンテンツが書き込まれる。端末14からコンテンツの書込要求を受信することにより、以下の処理が開始される。以下の処理は、大別して、前処理、メモリカードへの書き込み、ストレージサーバへの書き込みに分けることができる。

[0079] (2-2-1)前処理

ステップS301: CPU137の認証部は、端末14とチャレンジ・レスポンス型の認証を行う。

[0080] ステップS302: CPU137のアクセス制御部は、端末14からの読み出し依頼に応じ、マスタ鍵及びメディアIDをそれぞれROM134及び特殊領域138から読み出して端末14に渡す。

[0081] ステップS303: 前記認証処理で端末14との認証処理に成功している場合、CPU137のアクセス制御部は、端末14からの書込依頼に応じて暗号化キーを認証領域139bに書き込む。

[0082] ステップS304: CPU137のアクセス制御部は、端末14からの書込依頼に応じ、暗号化コンテンツを受け取り、RAM135に一時的に保存する。

[0083] (2-2-2)メモリカードへの書き込み

ステップS305: CPU137の空間統合部は、暗号化コンテンツをメモリカード13の非認証領域139cまたはストレージサーバ11の非認証領域111のいずれに書き込む

かを判断する。メモ리카ード13に書き込む場合にはステップS306に移行し、ストレージサーバ11に書き込む場合には後述するステップS309に移行する。

[0084] いずれに書き込むかの判断方法は特に限定されないが、以下のように行うことができる。例えば、端末14のユーザからいずれに書き込むかの指示を受け付け、その指示に従って書き込んでもよい。ユーザは、自分の使い勝手に合わせてデータを格納できるので便利である。

[0085] また、例えばいずれかを優先的な書込先とし、コンテンツを格納するのに十分な空き領域が優先的な書込先がない場合に他方の非認証領域に暗号化コンテンツを書き込んでもよい。この場合、空間統合部は、FAT139aとRAM135に保存されている暗号化コンテンツのデータ量とを比較し、空き領域の有無を確認した後に書込先を決定する。メモ리카ード13またはストレージサーバ11のいずれを優先的な書込先とするかは、予め決めておいても良いし、ユーザ設定可能にしてもよい。

[0086] さらに、データ量が空き領域に占める割合が小さくなる方の非認証領域を、書込先としてもよい。データ量に応じてデータの格納先を選択するので、記憶領域を効率的に使用することができる。

[0087] 前述の方法やその他のを適宜組み合わせて書込先を判断することもできる。いずれの判断方法を用いるかは、ユーザの利便性や記憶領域の効率性を考慮して決めればよい。

[0088] ステップS306～S308: CPU137のアクセス制御部は、暗号化コンテンツをメモ리카ード13上の非認証領域139cに書き込む(S306)。さらに、非認証領域139c中の一覧データに、新たに書き込んだコンテンツのレコードを追加する(S307)。最後にアクセス制御部は、フラッシュメモリ139のFAT139aを更新する。具体的には、アクセス制御部は、暗号化コンテンツのデータIDを、そのコンテンツを書き込んだアドレスに対応させてFAT139aに書き込み、処理を終了する(S308)。

[0089] (2-2-3) ストレージサーバへの書き込み

ステップS309～310: 暗号化コンテンツをストレージサーバ11に書き込むと判断した場合、アクセス制御部はストレージサーバ11に接続中か否かを判断する。接続中の場合、ステップS311に移行する。接続中でない場合にはネットワーク接続待機モ

ードに移行する。ネットワーク接続待機モード中にメモ리카ード13とストレージサーバ11との接続が確立された場合、ステップS311に移行する。

- [0090] ステップS311:CPU137のアクセス制御部は、後述する排他制御処理を実行し、その結果に基づいてストレージサーバ11への書込が可能か否かを判断する。この判断は、排他制御処理により前記録画処理許可フラグまたは編集処理許可フラグがON/OFFのいずれになったかに基づいて判断する。行おうとしている処理の許可フラグがOFFの場合は、ONになるまで待機する。待機せず、指定された書込処理が不可能である状態をユーザに通知して処理を終了してもよい。
- [0091] ステップS312:CPU137のアクセス制御部は、暗号化コンテンツを暗号・復号化回路1310及び無線通信部133を介し、ストレージサーバ11の非認証領域111に書き込む。この書込に先立ち、空間統合部は、ストレージサーバ11のURLと、非認証領域111のいずれのアドレスに暗号化コンテンツを書き込むかと、をアクセス制御部に指定する。アクセス制御部は、例えば接続情報中のURLと、HTTPの「PUSH」コマンドまたは「POST」コマンドと、RANGE指定子とを用いることにより、指定されたアドレスに暗号化コンテンツを書き込む。
- [0092] ステップS313:CPU137のアクセス制御部は、暗号・復号化回路1310及び無線通信部133を介し、ストレージサーバ11の非認証領域111中の一覧データに、新たに書き込んだコンテンツに関するレコードを追加する。追加に先立ち、空間統合部は、非認証領域111のいずれのアドレスに新たなレコードを書き込むかをアクセス制御部に指定する。
- [0093] ステップS314:CPU137の空間統合部は、アクセス制御部による書込が無事に終了後にメモ리카ード13内のFAT139aを更新する。これにより、ストレージサーバ11の非認証領域111に書き込まれたコンテンツ及び一覧データのデータIDと、非認証領域111中のアドレスとが、FAT139a内で対応付けて記憶される。
- [0094] 以上の処理により、端末14側の書込処理を変更することなく、メモ리카ード13内のフラッシュメモリ139のメモリ空間を広げることができる。また、ストレージサーバ11にコンテンツを書き込む場合であっても、暗号化キーと暗号化コンテンツとの保管場所が異なる。そのため、たとえ暗号化コンテンツが不当に入手されたとしても、暗号化キ

一が同時に不当に入手されないので、暗号化コンテンツの解読が不可能となり、コンテンツのセキュリティを保証することができる。

[0095] (3) 一覧出力処理

図11は、一覧出力処理における端末14側及びメモ리카ード13側の処理の流れの一例を示すフローチャートである。一覧出力処理は、コンテンツの読み出しに先立ち、コンテンツの概要の一覧を表示し、ユーザによるコンテンツの指定を受け付ける。

[0096] (3-1) 端末側の処理

まず、端末14側の一覧出力処理について説明する。端末14は、メモ리카ード13に対して一覧データを要求し、一覧データに基づく表示を行う。ユーザが画面上のボタンを押下するなどにより一覧出力要求が生じると、以下の処理が開始される。

[0097] ステップS401: 端末14のマイクロプロセッサ142は、ユーザからの要求に応じ、メモ리카ード13に対して一覧データを要求する。

[0098] ステップS402: 端末14のマイクロプロセッサ142は、前記要求に対し、メモ리카ード13から一覧データを取得する。

[0099] ステップS403: 端末14のマイクロプロセッサ142は、ディスプレイなどの出力装置15に対し、一覧データを出力する。これにより、前記図5に例示する画面が出力装置15上で表示される。

[0100] (3-2) メモ리카ード側の処理

次に、メモ리카ード13側における一覧出力処理について説明する。メモ리카ード13側では、端末14側からの一覧出力要求に応じ、メモ리카ード13内またはストレージサーバ11から一覧データを読み出し、端末14に出力する処理を行う。端末14から一覧出力要求を受け取ると、以下の処理が開始される。

[0101] ステップS501: CPU137のアクセス制御部は、メモ리카ード13内の非認証領域139cから一覧データを読み出し、RAM135に一時的に保存する。

[0102] ステップS502～S503: CPU137のアクセス制御部は、ストレージサーバ11に接続中か否かを判断する(S502)。接続中でない場合はネットワーク接続待機モードに移行する(S503)。ネットワーク接続待機モード中にメモ리카ード13とストレージサーバ11との接続が確立された場合、ステップS504に移行する。

- [0103] ステップS504ーS506:CPU137のアクセス制御部は、後述する排他制御処理を実行し(S504)、その結果に基づいてストレージサーバ11からの一覧データの読み出しが可能か否かを判断する(S505)。この判断は、排他制御処理において、再生処理許可フラグまたは追っかけ再生処理許可フラグのいずれかがONになったかどうかに基づいて行う。いずれの許可フラグもOFFの場合は、いずれかがONになるまで待機する(S506)。待機せず、一覧データの出力が不可能である状態をユーザに通知して処理を終了してもよい。
- [0104] ステップS507:CPU137のアクセス制御部は、ストレージサーバ11に蓄積されている一覧データの更新日時のうち最も新しいものD1を、ストレージサーバ11から読み出す。
- [0105] ステップS508:CPU137のアクセス制御部は、RAM135に保存しているメモリカード13の一覧データの更新日時のうち最も新しいものD2と、前記最終更新日時D1とを比較し、いずれの一覧データがより新しいかを決定する。
- [0106] ステップS509:ストレージサーバ11の一覧データの方が新しい場合、CPU137のアクセス制御部は、一覧データをストレージサーバ11から読み出す。この読み出しは、例えばバス146にストレージサーバ11のURL、HTTPのGETコマンド及びRANGE指定子を用いることで実行できる。RANGE指定子で指定するアドレスは、読み出しに先立ち、FAT139aを参照して取得する。
- [0107] さらにアクセス制御部は、ストレージサーバ11から取得した一覧データとRAM135に保存しているメモリカード13内の一覧データとをマージし、最新の一覧データを生成する。生成した一覧データはRAM135に上書きされる。
- [0108] ステップS510:CPU137のアクセス制御部は、RAM135の一覧データを端末14に送信する。また、アクセス制御部は、RAM135の一覧データを非認証領域139cの一覧データに上書きすることにより、メモリカード13の一覧データを最新の状態に更新する。
- [0109] 以上の処理により、最新の一覧データに基づく一覧出力が端末14で実行される。また、メモリカード13とストレージサーバ11とのそれぞれに記憶されている一覧データは、最新の状態に更新されてメモリカード13に記憶される。

[0110] (4) 読出処理

図12は、読出処理において端末14側及びメモリカード13側が行う処理の流れの一例を示すフローチャートである。この処理では、一覧出力画面で読出が指定されたコンテンツが、メモリカード13またはストレージサーバ11から読み出される。

[0111] (4-1) 端末側

端末14は、ユーザからコンテンツの指定を受け付け、指定されたコンテンツをメモリカード13から取得して出力する処理を行う。前記一覧出力処理において出力された一覧出力画面上でコンテンツが指定されると、以下の処理が開始される。

[0112] ステップS601: 端末14のマイクロプロセッサ142は、指定されたコンテンツのデータIDをメモリカード13に渡し、コンテンツの読出をメモリカード13に依頼する。

[0113] ステップS602～S604: 端末14のプロセッサは、メモリカード13の認証部との間で、チャレンジ・レスポンス型の認証を行う(S602)。その認証に成功すると、マスタ鍵・メディアID・暗号化キー・読出回数の読出をメモリカード13に依頼し、これらを取得する(S603、S604)。

[0114] ステップS605: 端末14のマイクロプロセッサ142は、読出回数に基づいて読出可能か否かを判断する。読出回数が“0”であれば、読出不可である。読出回数が1以上であれば、読出可能と判断する。

[0115] ステップS606: 端末14のマイクロプロセッサ142は、読出可能である場合、読出回数をインクリメントし、新たな読出回数の書込をメモリカード13に依頼する。以下の処理の実行により、残りの読出回数を1回減らすべきだからである。

[0116] ステップS607: 端末14のマイクロプロセッサ142は、メモリカード13から取得した暗号化キーをマスタ鍵及びメディアIDで復号化し、パスワードを抽出する。

[0117] ステップS608: 端末14のマイクロプロセッサ142は、メモリカード13から受信するコンテンツを前記パスワードで復号化しながら、出力装置15や記録媒体などに出力する。

[0118] (4-2) メモリカード側

メモリカード13は、端末14に指定されたコンテンツを、フラッシュメモリ139内の非認証領域139cまたはストレージサーバ11の非認証領域111から読み出し、端末14

に渡す。メモリカード13が端末14からコンテンツのデータIDと共に読出依頼を受け取ると、以下の処理が開始される。以下の処理は、前処理と、メモリカードからの読出と、ストレージサーバからの読出とに大別できる。

[0119] (4-2-1) 前処理

ステップS701: CPU137の認証部は、端末14とチャレンジ・レスポンス型の認証を行う。

[0120] ステップS702〜703: CPU137のアクセス制御部は、端末14との認証処理に成功している場合、端末14からの読み出し依頼に応じ、マスタ鍵・メディアID・暗号化キーを、それぞれROM134・特殊領域138・認証領域139bから読み出して端末14に渡す(S702)。また、読出回数を、認証領域139bから読み出して端末14に渡す(S703)。

[0121] ステップS704: CPU137のアクセス制御部は、端末14からの依頼に応じ、認証領域139bに記憶されている読出回数を更新する。

[0122] ステップS705: CPU137のアクセス制御部は、コンテンツのデータIDをキーにFATを検索し、コンテンツが記憶されているアドレスを取得する。

[0123] (4-2-2) メモリカードからの読み出し

ステップS706: CPU137の空間統合部は、アクセス制御部が取得したアクセス先のアドレスがメモリカード13かストレージサーバ11かを判断する。空間統合部は、アクセス先がストレージサーバ11である場合、NV-RAM136からストレージサーバ11のURLを読み出し、アクセス制御部に渡す。

[0124] ステップS707〜S708: アクセス先のアドレスがメモリカード13である場合、アクセス制御部は、アドレスに従って非認証領域139cにアクセスし、暗号化コンテンツを読み出す(S707)。読み出された暗号化コンテンツは、暗号・復号化回路1310で復号化され、端末14に送信される(S708)。

[0125] (4-2-3) ストレージサーバからの読み出し

ステップS709〜S710: アクセス先のアドレスがストレージサーバ11である場合、アクセス制御部はストレージサーバ11に接続中か否かを判断する(S709)。接続中の場合、後述するステップS711に移行する。接続中でない場合には、ネットワーク接

続待機モードに移行する(S710)。ネットワーク接続待機モード中にメモ리카ード13とストレージサーバ11との接続が確立された場合、ステップS711に移行する。

- [0126] ステップS711〜S713:アクセス先のアドレスがストレージサーバ11である場合、CPU137のアクセス制御部は、後述する排他制御処理を実行し(S711)、その結果に基づいてストレージサーバ11からの読み出しが可能か否かを判断する(S712)。この判断は、再生処理許可フラグまたは追っかけ再生処理許可フラグがONになっているか否かに基づいて行う。いずれの許可フラグもOFFの場合、いずれかの許可フラグがONになるのを待機する(S713)。待機せず、指定されたコンテンツの読出処理が不可能であることをユーザに通知して処理を終了してもよい。
- [0127] ステップS714:いずれかの許可フラグがONの場合、アクセス制御部は、ONとなっている許可フラグに応じ、ストレージサーバ11から暗号化コンテンツを取得する。すなわち、アクセス制御部は、ステップS705で取得したアドレスにアクセスし、暗号・復号化回路1310及び無線通信部133を介してストレージサーバ11から暗号化コンテンツを取得する。取得した暗号化コンテンツはRAM135に一時保存され、端末14に出力される(S708)。
- [0128] なお、再生処理許可フラグがONの場合は、アクセス制御部は、指定されたコンテンツを先頭アドレスから順次読み出せばよい。しかし、追っかけ再生処理許可フラグだけがONの場合、アクセス制御部は、指定されたコンテンツに対する書込アドレスを読出アドレスが追い越さないように読出を行う。後述するように、コンテンツは他のメモ리카ード13により録画されている最中だからである。
- [0129] 以上の処理では、端末14から読み出し要求を受けた場合、メモ리카ード13のCPU137はFATを参照し、データがメモ리카ード13かストレージサーバ11のどちらに蓄積されているかどうか判断する。ストレージサーバ11に蓄積されている場合、CPU137は、ストレージサーバ11からデータを読み出す。従って、ユーザは、メモ리카ード13さえあれば、コンテンツをメモ리카ード13からはもちろんストレージサーバ11からも読み出すことができるので、メモ리카ード13の見かけ上の記憶容量が増大したように感じる。
- [0130] しかも、著作権で保護されているコンテンツを暗号化するためのパスワードと暗号化

コンテンツとを別々の場所に記憶することで、たとえ暗号化コンテンツが不当に入手されたとしても、暗号化キーが同時に不当に入手されるのを防ぎ、コンテンツのセキュリティを保証することができる。

[0131] (5)排他制御処理

図13は、メモリカード13が行う排他制御処理の流れの一例を示すフローチャートである。この処理では、他のメモリカード13がストレージサーバ11上の同一のアクセス対象にアクセスしようとしている場合に、同一のアクセス対象への書込または読出に一定の制限を加える。より具体的には、この処理では、ストレージサーバ11へのアクセスが生じるたびに、以下の処理が開始される。

[0132] ステップS801:競合判断部は、生じたアクセスが読出処理なのか、書込処理なのかを判断する。ここでは読出処理として再生処理を、書込処理として録画処理または編集処理を考える。

[0133] ステップS802:競合判断部は、読出処理が生じた場合、読出対象が他のメモリカード13により編集処理中か否かを判断する。この判断は、ストレージサーバ11側に同時接続数を問い合わせ得られる応答に基づいて行うことが出来る。

[0134] ステップS803:読出対象が他のメモリカード13により編集中である場合、競合判断部は再生処理許可フラグ及び追っかけ再生許可フラグをともにOFFにする。この場合、「編集中のため、再生できません」などのメッセージを端末14に出力する。これから再生しようとしている対象データが、他の半導体メモリカード13からのアクセスによって再生中に書き換えられることを防止することができる。

[0135] ステップS804:読出対象が他のメモリカード13により編集中ではない場合、競合判断部は読出対象が他のメモリカード13により録画処理中か否かをさらに判断する。

[0136] ステップS805:読出対象が他のメモリカード13により録画処理中でない場合、競合判断部は再生処理許可フラグをONに設定する。

[0137] ステップS806:読出対象が他のメモリカード13により録画処理中である場合、競合判断部は追っかけ再生処理許可フラグをONに設定する。読出アドレスが録画のための書込アドレスを追い越さない範囲で再生を許可するためである。アクセス制御部は、追っかけ再生処理許可フラグに基づいて追っかけ再生中に、早送り操作により

録画のための書込アドレスに読出アドレスが近づいた場合、早送りを解除して等速再生に移行することもできる。

[0138] ステップS807:前記ステップS801で生じたアクセスが書込処理と判断した場合、競合判断部はさらに、書込処理が編集処理なのか録画処理なのかを判断する。

[0139] ステップS808:録画処理のためのアクセスが生じた場合、競合判断部は録画処理許可フラグをONに設定する。新規にデータを書き込む場合には、他のメモ리카ード13との競合は生じないからである。

[0140] ステップS809:編集処理のためのアクセスが生じた場合、競合判断部は編集対象が他のメモ리카ード13からのアクセスにより、録画・編集・再生のいずれかの処理中か否かを判断する。

[0141] ステップS810:競合判断部は、編集対象に対し何らかの処理が施されている間、その処理が終了するまで編集処理許可フラグをOFFに設定し、処理が終了すると編集処理許可フラグをONに変更する。

[0142] ステップS811:競合判断部は、編集対象に対し他のメモ리카ード13からのアクセスがない場合、編集処理許可フラグをONに設定する。これにより、これから編集しようとしている対象データが他のメモ리카ード13からのアクセスによって書き換えられることを防止できる。

[0143] 以上の処理により、ストレージサーバ11上の同一のデータに複数のメモ리카ード13からアクセスした場合に生じうる競合を回避することができる。

[0144] [効果]

以上述べたように、本発明のメモ리카ード13は、無線通信部133及び接続部を有しているので、ネットワーク上のストレージサーバ11にアクセス可能である。ストレージサーバ11上に非認証領域や認証領域を設け、メモ리카ード13内のフラッシュメモリ139と統合したメモリ空間としてメモ리카ード13内で管理することで、メモ리카ード13のメモリ空間を見かけ上増加させることができる。このように増築されたメモリ空間は、メモ리카ード13さえあれば任意の端末14からアクセスできるので、大量のデータを格納したいユーザにとって利便性と自由度が向上する。

[0145] さらに、著作権で保護された暗号化コンテンツをストレージサーバ11に、その復号

化に必要な暗号キーをメモリカード13に格納しておけば、仮に暗号化コンテンツが第3者により不当に入手されても、コンテンツのセキュリティを保証することができる。

[0146] <その他の実施形態>

(A) 前記第1実施形態のシステムは1つのストレージサーバ11だけを含んでいるが、複数のストレージサーバ11a, b...を含んでも良い。その場合、メモリカード13のFATは、メモリカード13内のメモリ空間に加え、各ストレージサーバ11a, b...の記憶領域のアドレスを管理する。また、FATは、どのストレージサーバ11にどのアドレス空間を割り当てているかを管理する。NV-RAM136には、各ストレージサーバ11のネットワークアドレスが記憶されている。

[0147] (B) 前記第1実施形態では、認証領域をメモリカード13にのみ設けているが、認証領域(第2認証領域に相当)をストレージサーバ11上に設けることもできる。認証領域をストレージサーバ11に設けることにより、メモリカード13中の認証領域をも見かけ上増大させることができる。従って、例えばコンテンツなどのデータを暗号化せずにメモリカード13上の認証領域またはストレージサーバ11上の認証領域に格納しても記憶領域を十分に準備でき、かつコンテンツのセキュリティを保証することができる。

[0148] (C) 前記第1実施形態では、メモリカード13の無線通信部133及び接続部の機能を用いてストレージサーバ11とメモリカード13との接続を確立している。しかし、端末14に通信機能がある場合、端末14側通信機能を用いてストレージサーバ11とメモリカード13との接続を確立してもよい。どちらの通信機能を用いるかは、通信費用や通信速度を勘案して自動的に決定することができる。

[0149] (D) 前記メモリカード13に各種のユーザ設定を記憶させておき、任意の端末14でそのユーザ設定を使用することもできる。例えば、ユーザインターフェースのカラー設定、ユーザ名表記、利き腕などのユーザ設定をメモリカード13に記憶させることで、ユーザは自分が所有する端末14以外の端末14であっても、いつも使用している設定と同じ設定で端末14を使用することができる。

[0150] (E) ストレージサーバ11へのアクセス時に、ストレージサーバ11が接続用識別IDを単位としてアクセス権を管理してもよい。図14に、アクセス権管理がある場合の番組一覧表示画面例を示す。また図15に、ストレージサーバ11が保持するアクセス権管

理テーブルのデータ例を示す。さらに図16に、ストレージサーバ11に対し、異なるアクセス権でアクセス可能なメモリカード13を作成するための画面例を示す。

[0151] データファイルに対するアクセス権管理については、コンピュータにおけるファイルシステムを用いたアクセス権管理などにおいて一般的な技術を適用可能である。

[0152] (F)着脱可能な半導体メモリカードとしては、メモリカードに限らず、可搬性がある記録媒体であり、ネットワーク上の蓄積装置にアクセスし、記録媒体のメモリ空間と蓄積装置のメモリ空間とを統合可能な空間統合手段を有するものであればよい。他の例としては、リムーバブルHDDユニット、カートリッジに本願発明の制御機構と共に格納された光ディスクを挙げることができる。

[0153] (G)本発明の基本概念は、半導体を用いた記録媒体だけでなく、光学方式、磁気方式またはバイオ技術を応用した記録媒体にも適用可能である。

[0154] (H)前述した半導体メモリカードが実行する方法を実行するためのプログラムは、本発明の範囲に含まれる。また、そのプログラムを記録したコンピュータ読み取り可能な記録媒体も本発明の範囲に含まれる。ここで記録媒体としては、コンピュータが読み書き可能なフレキシブルディスク、ハードディスク、半導体メモリ、CD-ROM、DVD、光磁気ディスク(MO)、その他のものが挙げられる。またプログラムには、記録媒体に記憶されているものもダウンロード可能なものが含まれる。

産業上の利用可能性

[0155] 本発明は、持ち運びが可能であり、電子機器に挿入してデータの書込や読み出しを行う可搬型記録媒体に適用可能である。

請求の範囲

- [1] 電子機器に着脱可能な半導体メモリカードであって、
書き換え可能な第1不揮発性メモリと、
前記第1不揮発性メモリへの前記電子機器によるアクセスを制御する第1アクセス制御手段と、
書き換え可能な第2不揮発性メモリを有するネットワーク上の蓄積装置への前記電子機器によるアクセスを制御する通信手段と、
前記第2不揮発性メモリへの前記電子機器によるアクセスを制御する第2アクセス制御手段と、
前記第1不揮発性メモリ及び前記第2不揮発性メモリを含む擬似統合メモリ空間を生成する空間統合手段と、
を含むことを特徴とする半導体メモリカード。
- [2] 前記第2アクセス手段によりアクセスしようとするデータが他の半導体メモリカードにより書込または読出中か否かを判断し、判断結果に応じて前記第2アクセス手段による書込及び／または読出を開始、中止または遅延させる競合判断手段をさらに備えることを特徴とする、請求項1に記載の半導体メモリカード。
- [3] 前記通信手段は、前記蓄積装置の前記ネットワーク上でのアドレスを記憶していることを特徴とする、請求項1に記載の半導体メモリカード。
- [4] 前記通信手段は、半導体メモリカードの識別情報を用いて前記蓄積装置にアクセスすることを特徴とする、請求項3に記載の半導体メモリカード。
- [5] 前記データを暗号化するための暗号化キーを生成し、前記暗号化キーで前記データを暗号化する暗号化手段と、
前記電子機器の正当性を検証する認証手段と、をさらに有し、
前記第1不揮発性メモリは、予め定められた記憶領域である第1認証領域と第1非認証領域とを含み、
前記第1アクセス手段は、前記第1非認証領域への前記電子機器によるアクセスを制御し、前記認証手段が前記電子機器の正当性を認証した場合に前記第1認証領域への前記電子機器によるアクセスを許可し、

前記第2アクセス手段は、前記第2不揮発性メモリに含まれ予め定められた記憶領域である第2非認証領域への前記電子機器によるアクセスを制御し、

前記空間統合手段は、前記第2不揮発性メモリ内の第2非認証領域のアドレスを前記暗号化キーで暗号化された前記データに割り当て、前記第1不揮発性メモリ内の第1認証領域のアドレスを前記暗号化キーに割り当てることを特徴とする、請求項1に記載の半導体メモリカード。

- [6] 前記空間統合手段は、前記第1不揮発性メモリ内の第1非認証領域または前記第2不揮発性メモリ内の第2非認証領域のいずれのアドレスを前記暗号化キーで暗号化されたデータに割り当てるかを判断し、前記判断に従って前記データへのアドレスの割り当てを行うことを特徴とする、請求項5に記載の半導体メモリカード。
- [7] 前記第2アクセス手段は、前記認証手段が前記電子機器の正当性を認証した場合、前記第2不揮発性メモリ内の予め定められた記憶領域である前記第2認証領域への前記電子機器によるアクセスを許可することを特徴とする、請求項5に記載の半導体メモリカード。
- [8] 前記第1不揮発性メモリは管理領域を含み、
前記空間統合手段は、前記第1不揮発性メモリまたは前記第2不揮発性メモリ中のアドレスをデータに割り当て、前記データを識別するデータ識別子と前記割り当てたアドレスと対応づけて前記管理領域に書き込み、
前記第1アクセス手段及び前記第2アクセス手段は、前記第1不揮発性メモリまたは前記第2不揮発性メモリへの前記データの書き込み要求を受け付け、前記データに割り当てられたアドレスに対応する記憶領域に前記データを書き込むことを特徴とする、請求項1に記載の半導体メモリカード。
- [9] 前記第2アクセス手段は、データの読み出し要求を受け付け、前記データが書き込まれている第2不揮発性メモリのアドレスを前記管理領域から読み出し、読み出したアドレスに前記通信手段を介してアクセスして前記データを読み出すことを特徴とする、請求項8に記載の半導体メモリカード。
- [10] 前記データを暗号化及び復号化するための暗号化キーを生成し、前記暗号化キーで前記データを暗号化する暗号化手段をさらに有し、

前記第2アクセス手段は、前記暗号化キーで暗号化されたデータが書き込まれている前記第2非認証領域のアドレスを前記管理領域から読み出し、前記第2非認証領域の前記アドレスにアクセスして暗号化された前記データを前記通信手段を介して読み出し、

前記第1アクセス手段は、前記暗号化キーが書き込まれている第1認証領域のアドレスを前記管理領域から読み出し、前記第1認証領域の前記アドレスにアクセスして前記暗号化キーを読み出すことを特徴とする、請求項8に記載の半導体メモリカード。

[11] 書き換え可能な第1不揮発性メモリへの電子機器によるアクセスを制御する第1アクセス制御ステップと、

書き換え可能な第2不揮発性メモリを有するネットワーク上の蓄積装置への前記電子機器によるアクセスを制御する通信ステップと、

前記第2不揮発性メモリへの前記電子機器によるアクセスを制御する第2アクセス制御ステップと、

前記第1不揮発性メモリ及び前記第2不揮発性メモリを含む擬似統合メモリ空間を生成する空間統合ステップと、

を含むことを特徴とするメモリ空間管理方法。

[12] 電子機器に着脱可能でありコンピュータを含む半導体メモリカードに記録されたメモリ空間管理プログラムであって、

書き換え可能な第1不揮発性メモリへの前記電子機器によるアクセスを制御する第1アクセス制御手段、

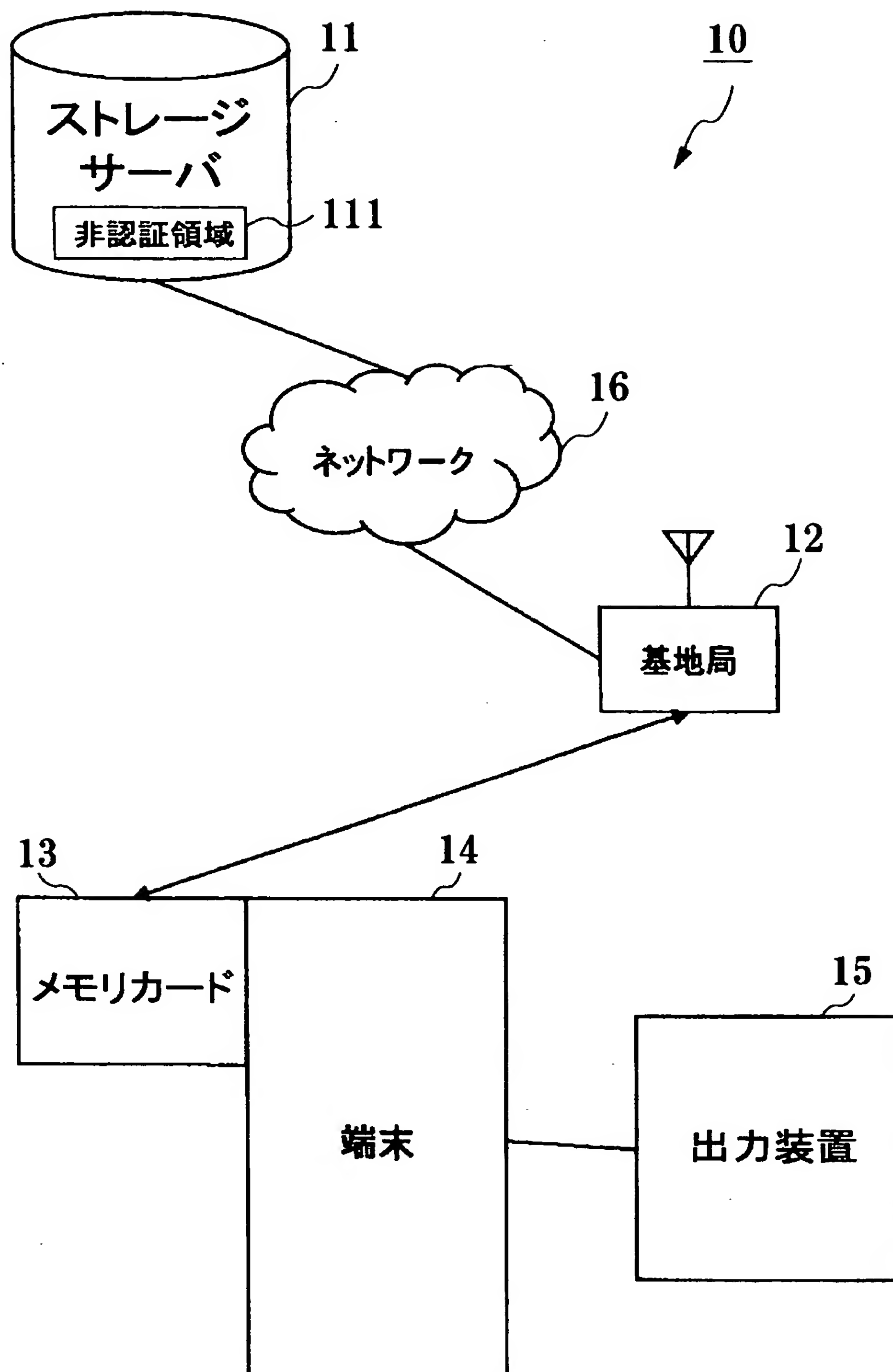
書き換え可能な第2不揮発性メモリを有するネットワーク上の蓄積装置への前記電子機器によるアクセスを制御する通信手段、

前記第2不揮発性メモリへの前記電子機器によるアクセスを制御する第2アクセス制御手段、及び

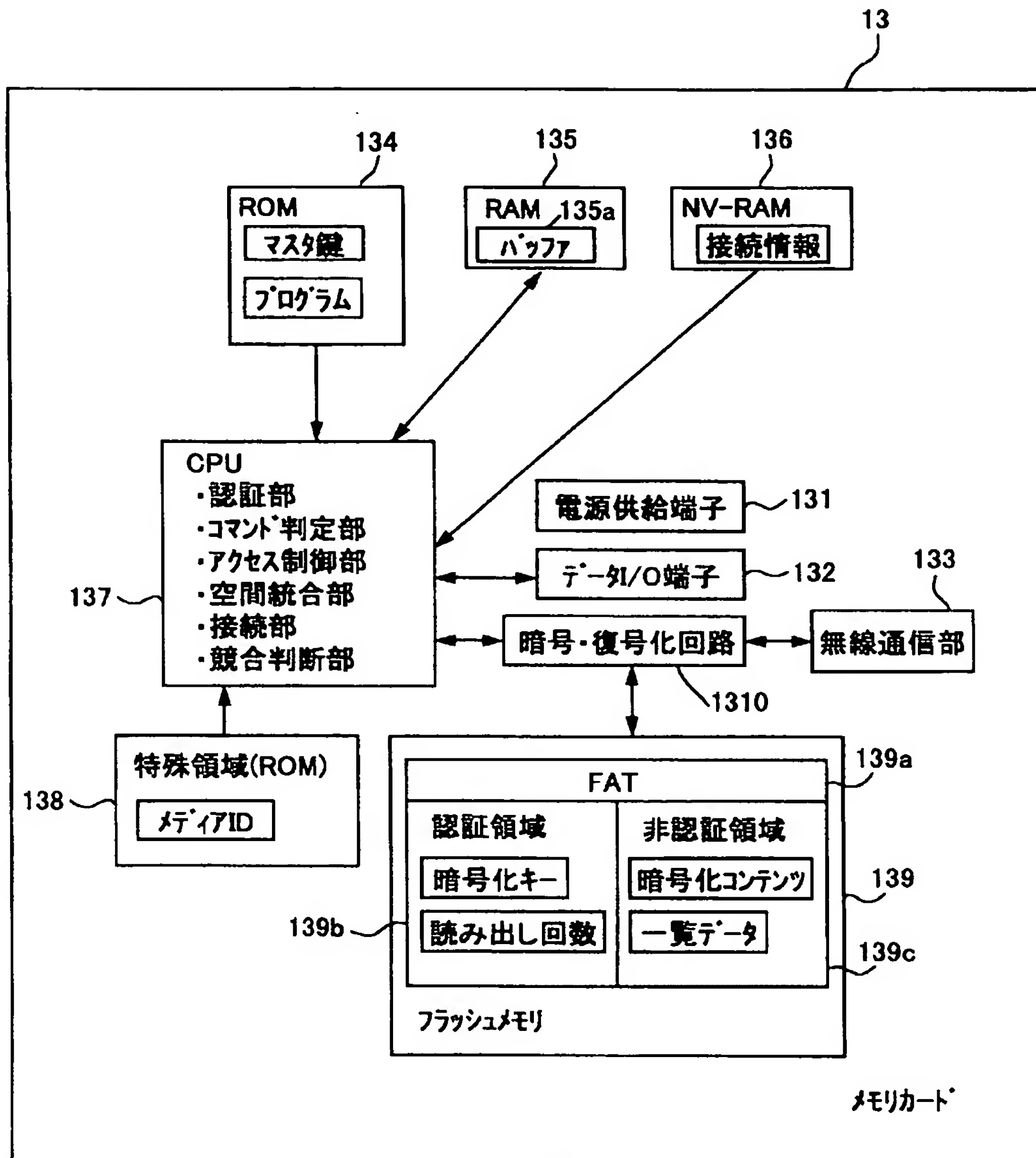
前記第1不揮発性メモリ及び前記第2不揮発性メモリを含む擬似統合メモリ空間を生成する空間統合手段、

として前記コンピュータを機能させる、メモリ空間管理プログラム。

[図1]



[図2]



[図3]

接続情報(NV-RAM)

136

接続先URL	http://storage.server.com/rm/login.asp
接続用識別ID	301938472G322DPE
接続認証パスワード	F32248DCPDCL20EM

[図4]

139c

一覧用データファイル					
最終更新日時			03/10/15/20:12:00		
⋮					
Ch	録画日	時刻	画質	録画時刻	保護
BS 7	03/10/10	19:00	SP	01:00	無し
映像データファイル名				タイトル	
/DVD_RTAV/MOV00011.MPG				BSスペシャル	
⋮					
Ch	録画日	時刻	画質	録画時刻	保護
12	03/10/10	14:00	SP	01:24	無し
映像データファイル名				タイトル	
/DVD_RTAV/MOV00012.MPG				サッカー中継	
⋮					
Ch	録画日	時刻	画質	録画時刻	保護
12	03/10/11	21:00	SP	00:28	無し
映像データファイル名				タイトル	
/DVD_RTAV/MOV00013.MPG				音楽特集	
⋮					

[図5]

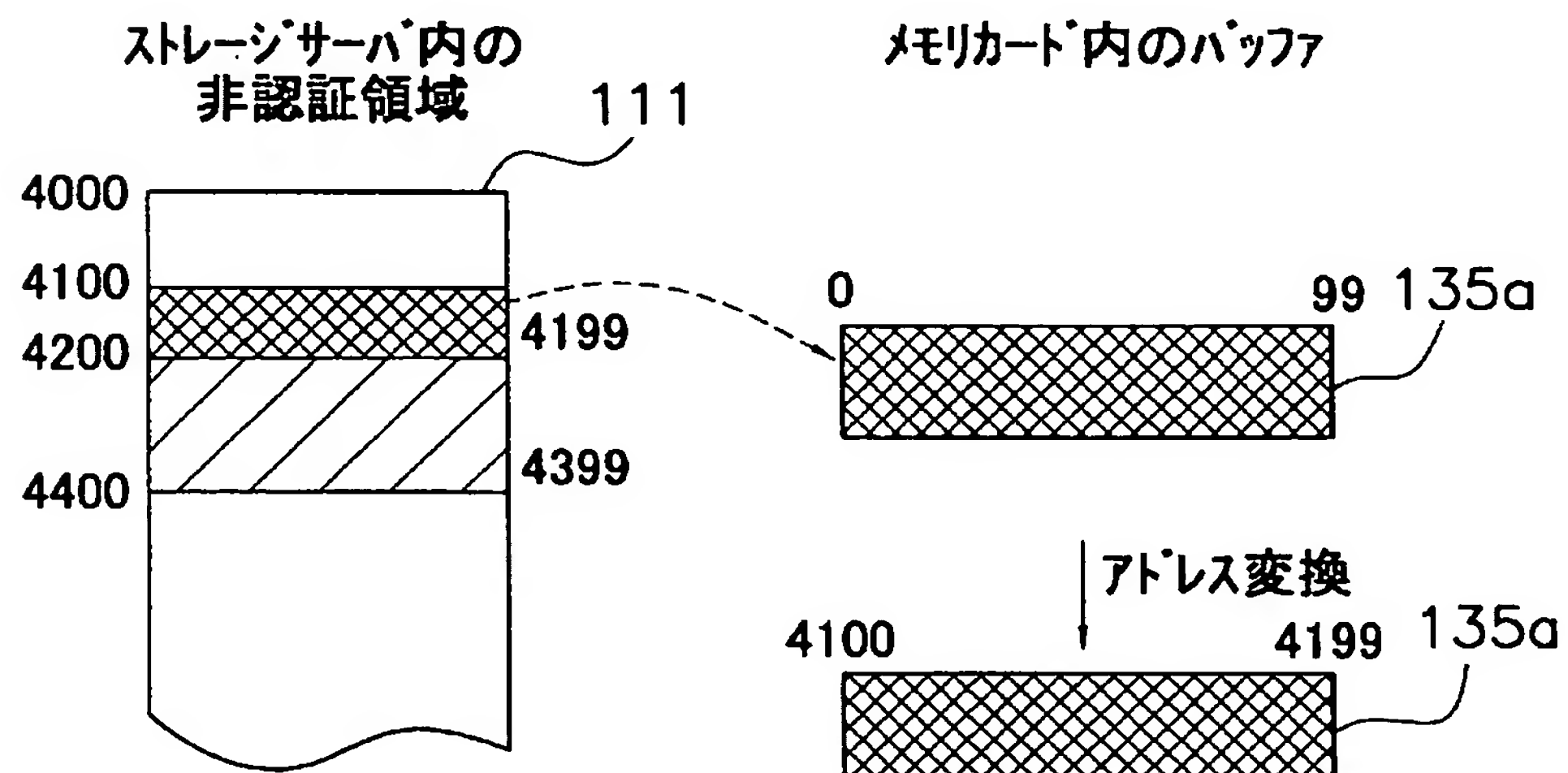
						701
プログラムナビ			SD			
<div></div>	No	Ch	録画日	時刻	タイトル	
	005	BS 7	03/10/10	19:00	BSスペシャル	
	006	12	03/10/10	14:00	サッカー中継	
	007	12	03/10/11	21:00	音楽特集	
	008	4	03/10/13	19:00	歴史特集	

[図6]

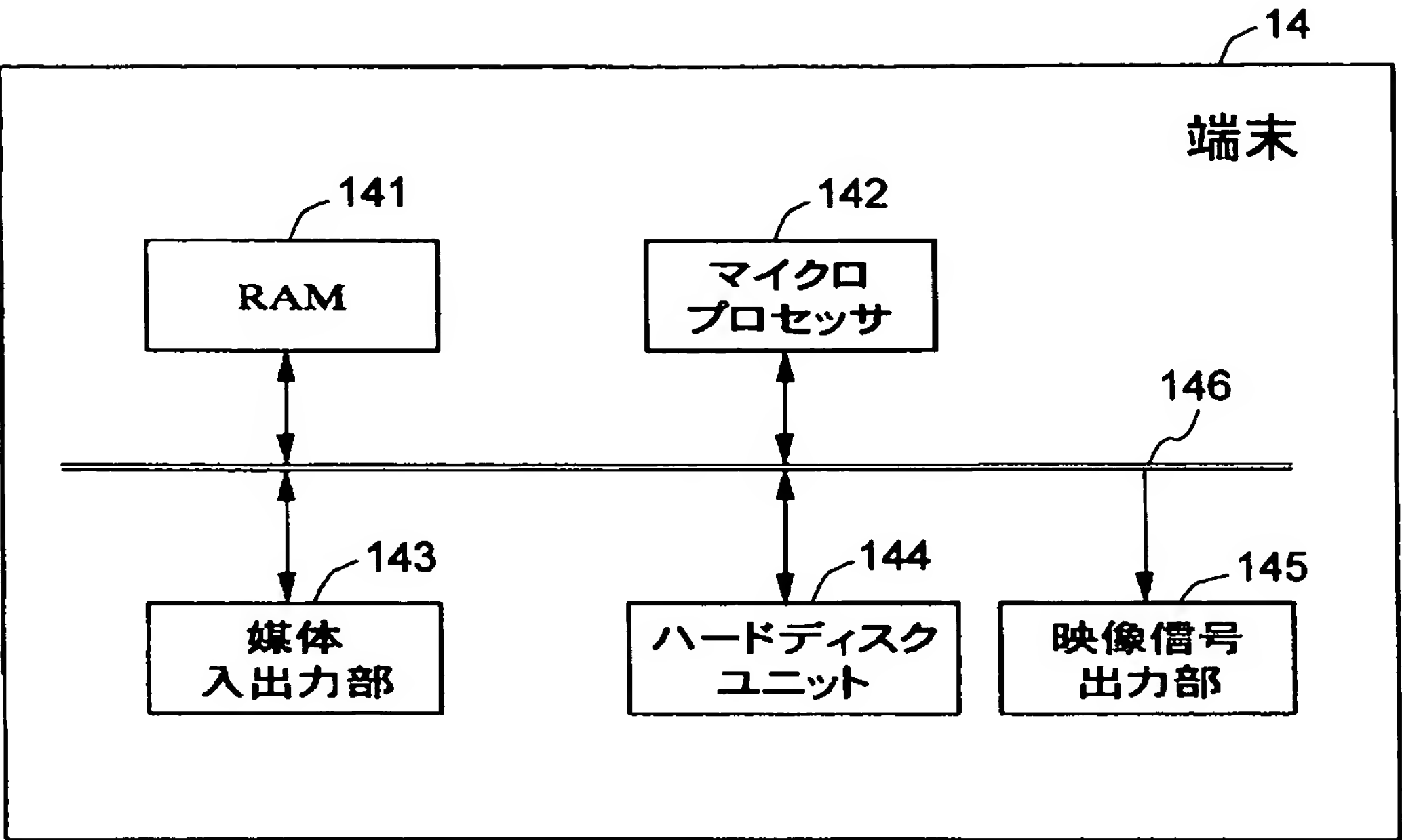
FAT 139a

	アドレス	データID
認証領域	0000	ENCRYPT/MOV00011.MPG
	⋮	⋮
	0100	ENCRYPT/MOV00012.MPG
非認証領域	⋮	⋮
	3000	DVD_RTAV/MOV00011.MPG
	⋮	⋮
非認証領域 (サーバ)	4000	DVD_RTAV/MOV00012.MPG
	⋮	⋮

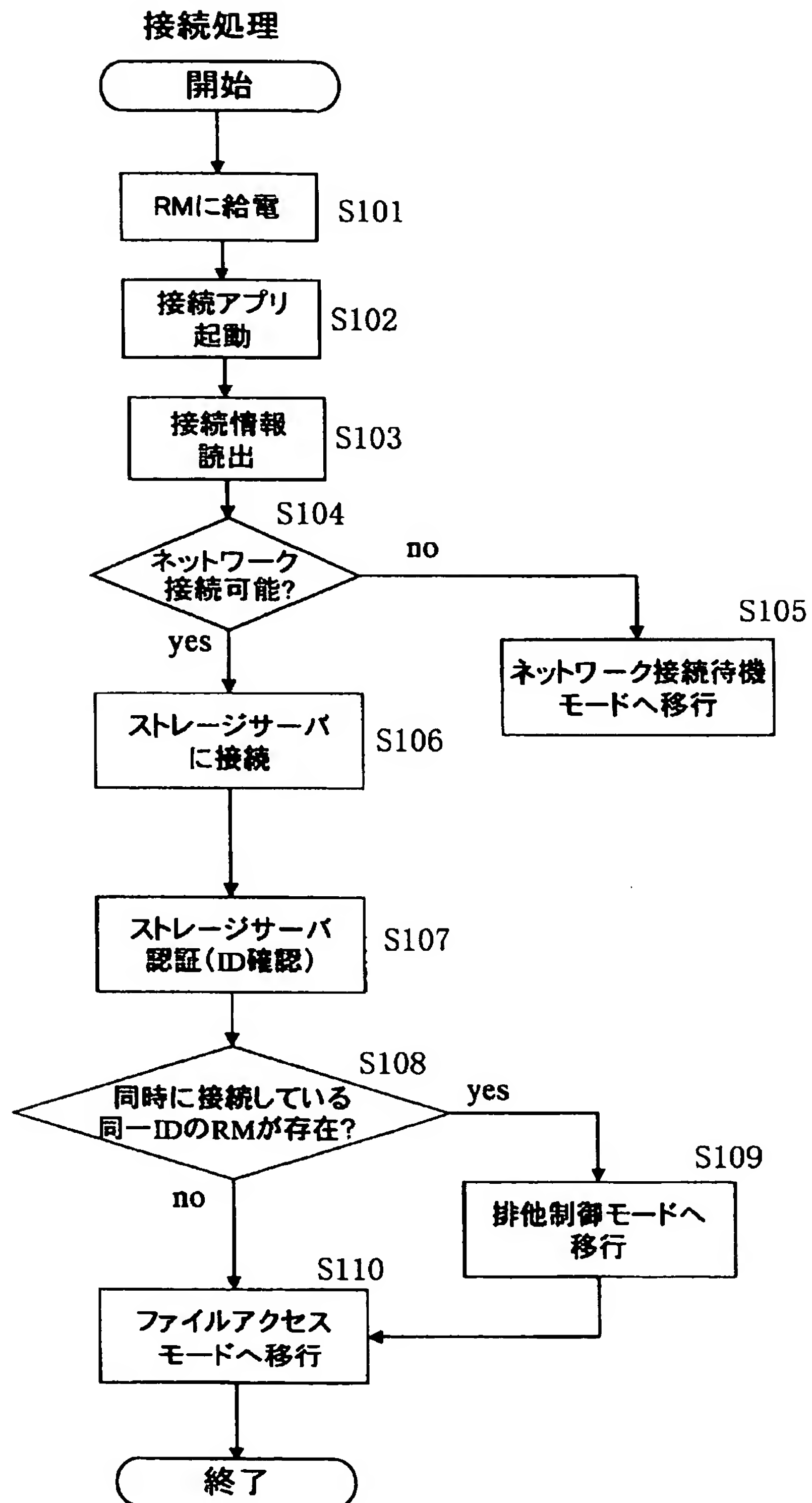
[図7]



[図8]

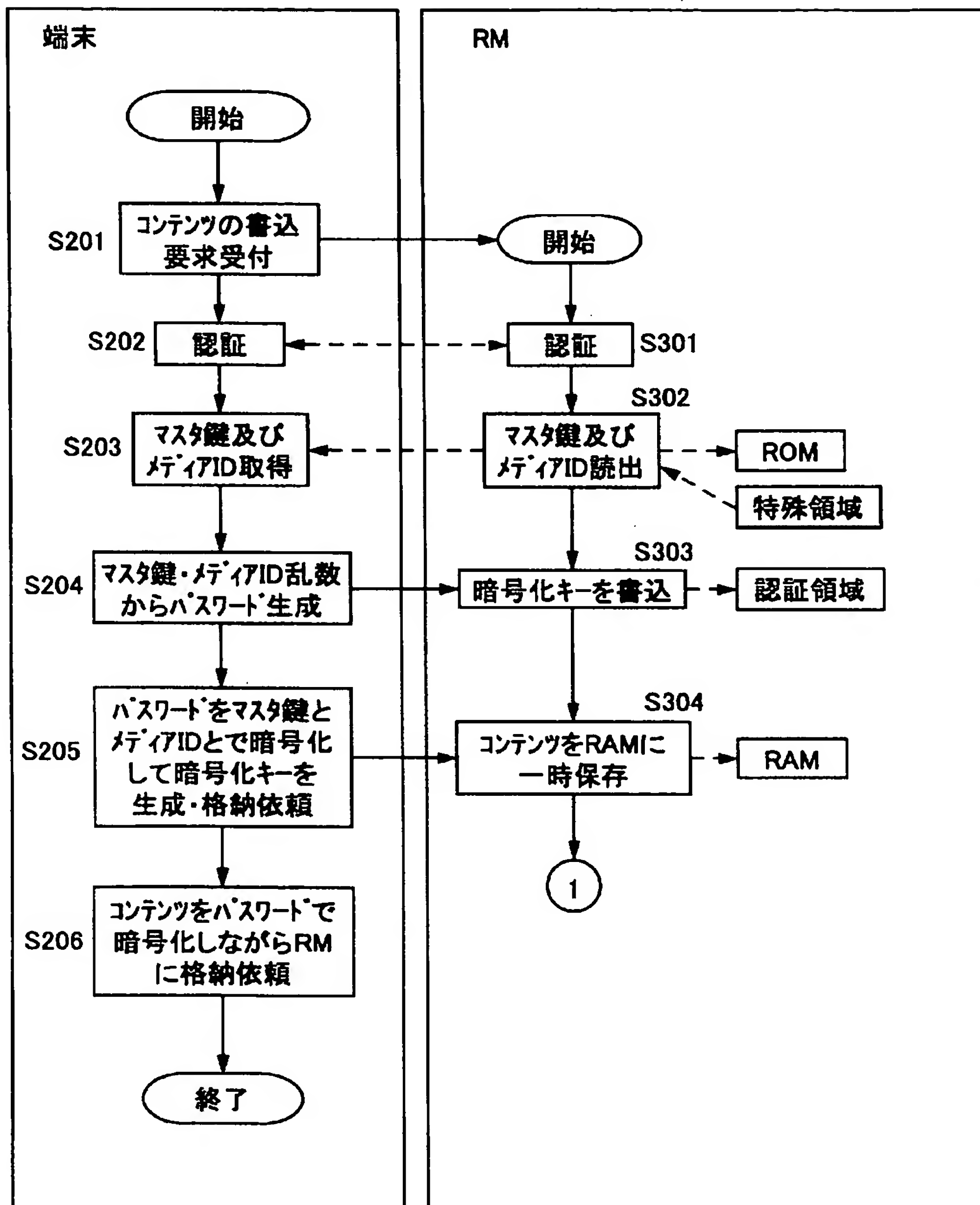


[図9]



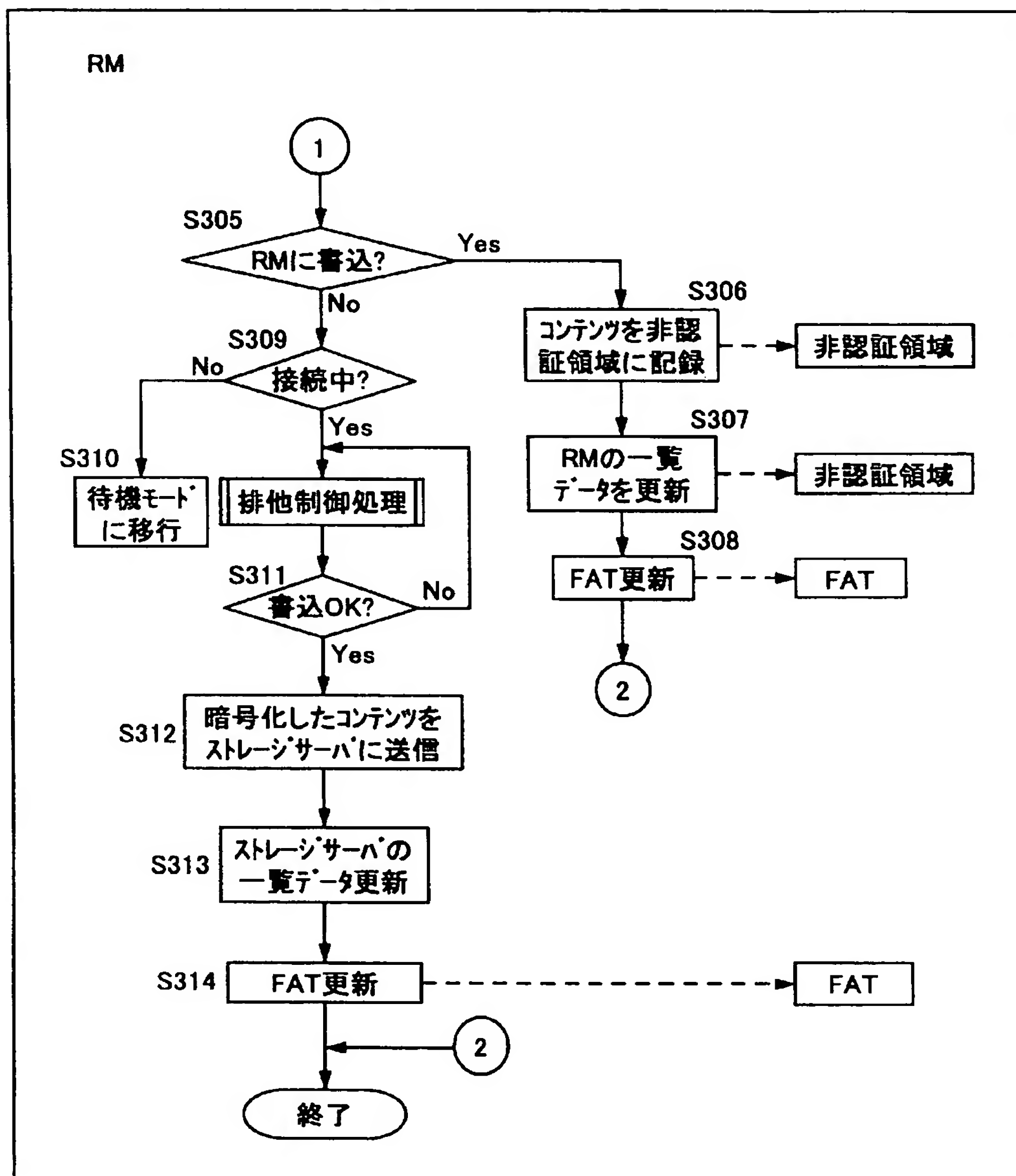
[図10A]

書込処理



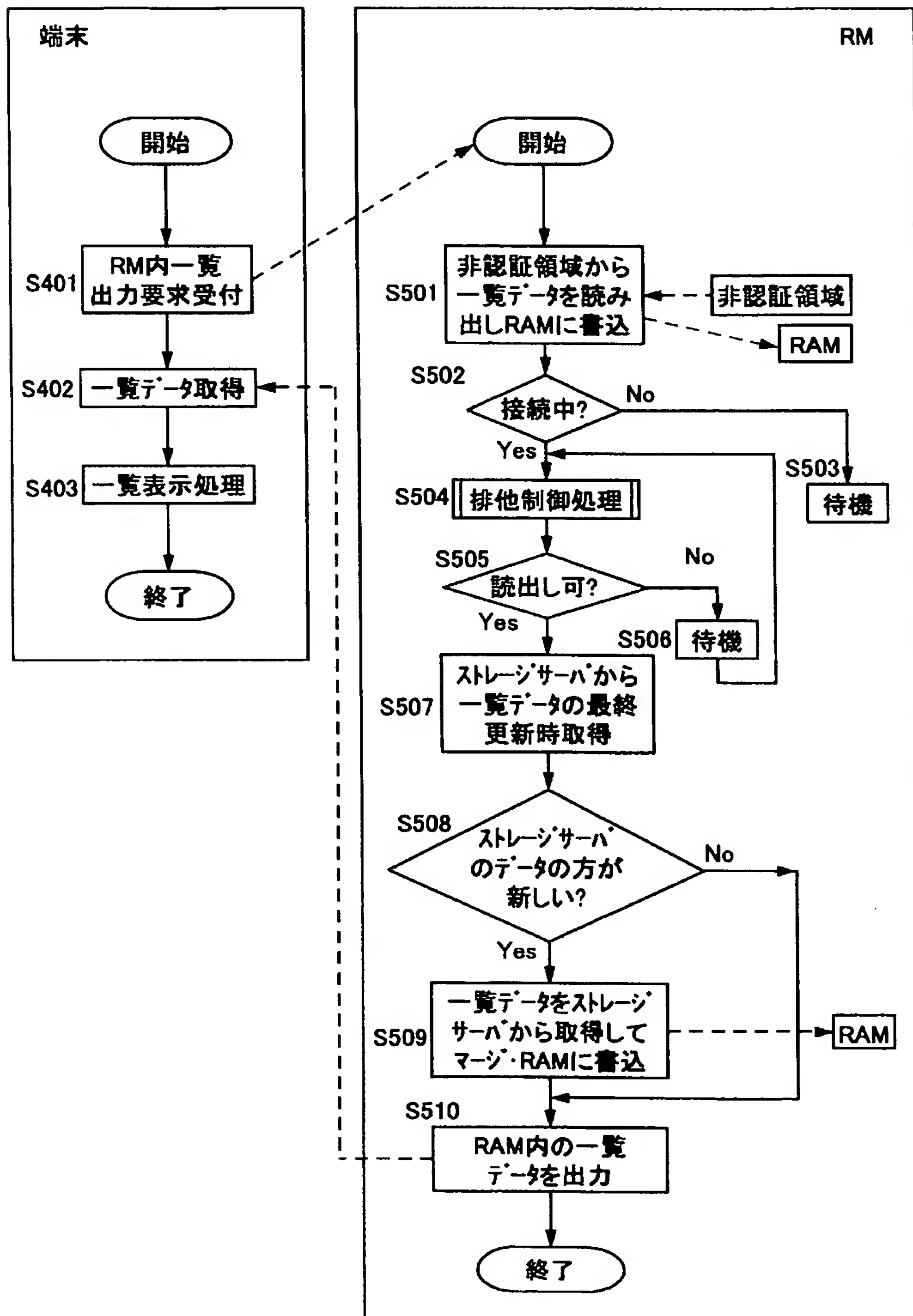
[図10B]

書込処理



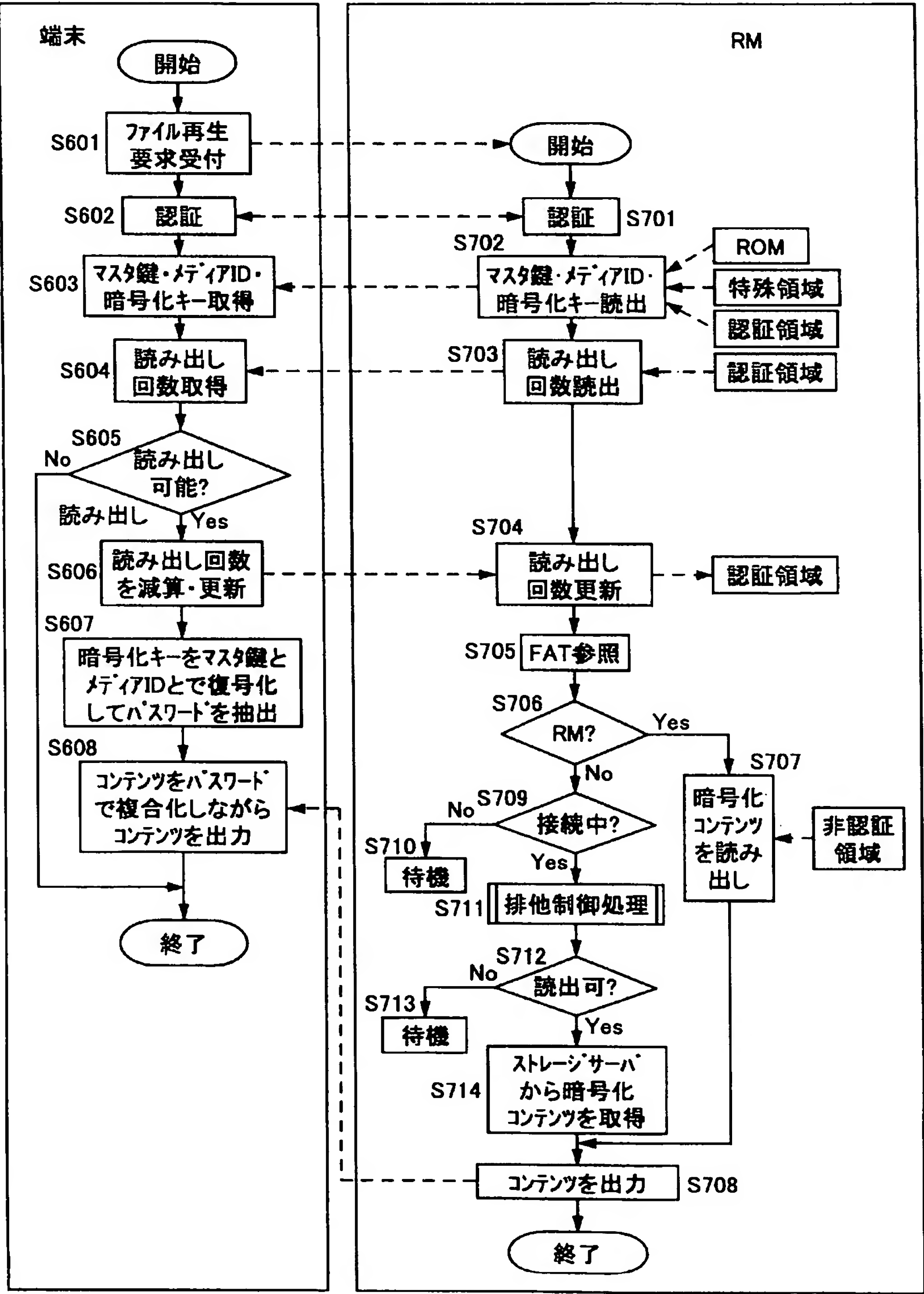
[図11]

一覧出力処理

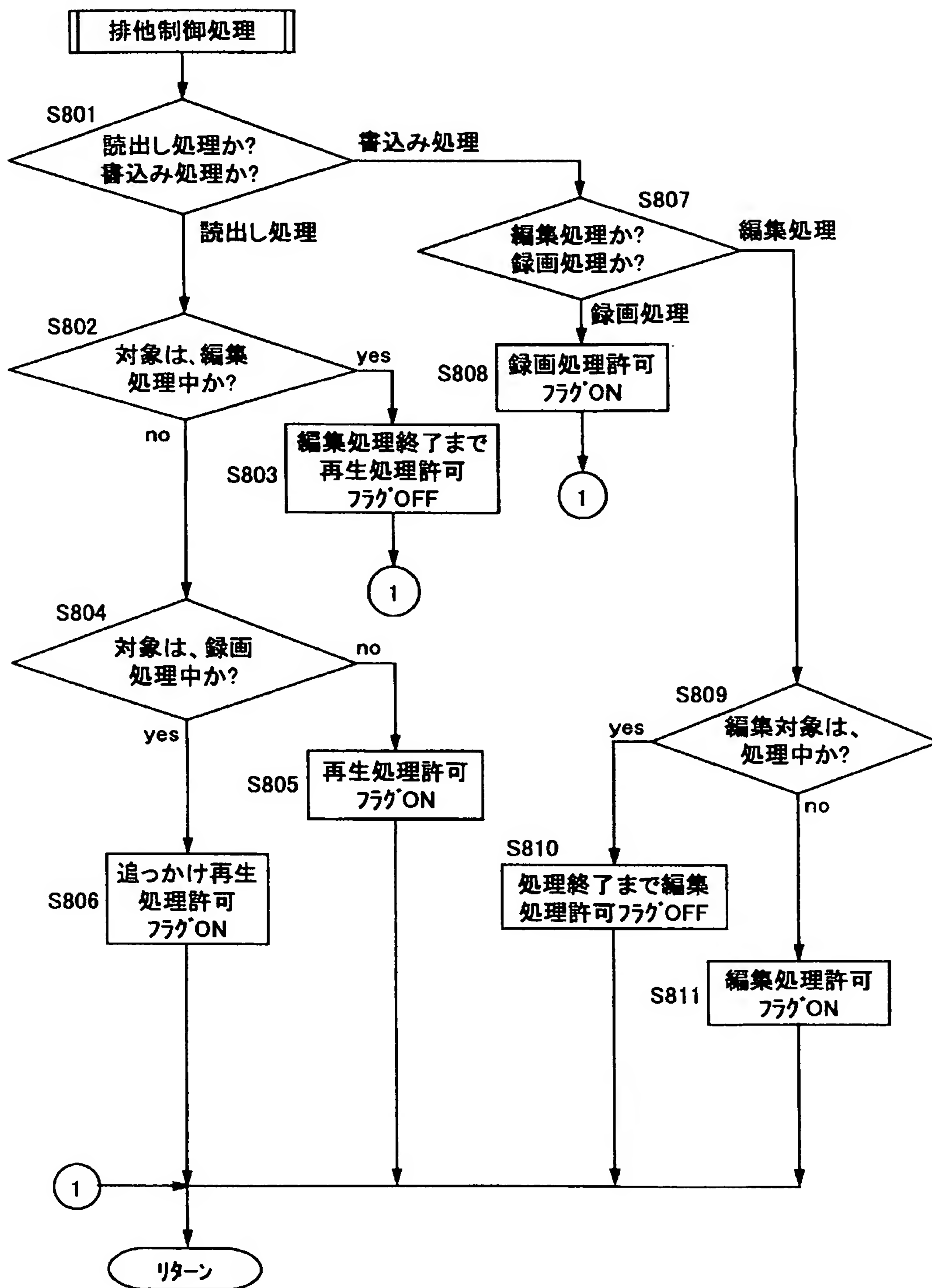


[図12]






読出処理



[図13]



[図14]

プログラムナビ			SD		ユーザ名:○○○	
    	No	Ch	録画日	時刻	タイトル	アクセス権
	005	BS 7	03/10/10	19:00	BSスペシャル	Full
	006	12	03/10/10	14:00	サッカー中継	Read only
	007	12	03/10/11	21:00	音楽特集	Full
	008	4	03/10/13	19:00	歴史特集	Non access

[図15]

ユーザ管理テーブル	
最終更新日時	03/10/15/20:12:00
⋮	
グループID	0549SDG6EG35
アクセス可能リムーバブルメディア	
接続用識別ID	301938472G322DPE
接続認証パスワード	F32248DCPDCL20EM
アクセス権	All
接続用識別ID	DK937546ED354984
接続認証パスワード	DKPE03KDUI38DUOL
アクセス権	User: Mike
接続用識別ID	6584316E8D4Q6545
接続認証パスワード	DKUE69dje36423di
アクセス権	Guest
⋮	
⋮	

[図16]

ダビング	SD→SD
作成するSDの、アクセス権を選択してください	
アクセス権	説明
ALL	すべてのデータを再生・削除・編集できます
Guest	Guest向けに許可されたデータの再生のみが可能です
User:Mike	Guest向けに許可されたデータの再生と、Mike用データの再生・削除・編集ができます
User:Mary	Guest向けに許可されたデータの再生と、Mary用データの再生・削除・編集ができます
<div>新規Userの作成</div>	

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/016954

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ G06F12/00, 12/14, H04L29/02, G06K19/073

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ G06F12/00, 12/14, H04L29/02, G06K19/00-19/10

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2005
Kokai Jitsuyo Shinan Koho	1971-2005	Toroku Jitsuyo Shinan Koho	1994-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2002-99475 A (Toshiba Corp.), 05 April, 2002 (05.04.02), Full text; all drawings & EP 1191451 A2 & US 2002/0037745 A1	1-12
A	JP 2003-110976 A (Fuji Photo Film Co., Ltd.), 11 April, 2003 (11.04.03), Full text; all drawings & EP 1298914 A2 & US 2003/0077064 A1	1-12
A	JP 2000-115253 A (Toshiba Corp.), 21 April, 2000 (21.04.00), Full text; all drawings & US 6643284 B1	1-12

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance
 "E" earlier application or patent but published on or after the international filing date
 "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
 "O" document referring to an oral disclosure, use, exhibition or other means
 "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
 "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
 "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
 "&" document member of the same patent family

Date of the actual completion of the international search
15 February, 2005 (15.02.05)

Date of mailing of the international search report
08 March, 2005 (08.03.05)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int.Cl⁷. G 0 6 F 1 2 / 0 0, 1 2 / 1 4, H 0 4 L 2 9 / 0 2, G 0 6 K 1 9 / 0 7 3

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int.Cl⁷. G 0 6 F 1 2 / 0 0, 1 2 / 1 4, H 0 4 L 2 9 / 0 2, G 0 6 K 1 9 / 0 0 - 1 9 / 1 0

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2005年
日本国実用新案登録公報	1996-2005年
日本国登録実用新案公報	1994-2005年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X.	J P 2002-99475 A (株式会社東芝) 2002.04.05, 全文, 全図 & E P 1191451 A2 & U S 2002/0037745 A1	1-12
A	J P 2003-110976 A (富士写真フイルム株式会社) 2003.04.11, 全文, 全図 & E P 1298914 A2 & U S 2003/0077064 A1	1-12

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日

15.02.2005

国際調査報告の発送日

08.3.2005

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)
郵便番号100-8915
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

相崎 裕恒

5 N

9290

電話番号 03-3581-1101 内線 3585

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	J P 2000-115253 A (株式会社東芝) 2000.0 4.21, 全文, 全図 & US 6643284 B1	1-12